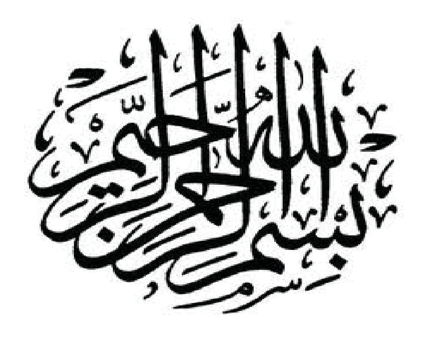
الجرائم الإلكترونية

ماهيتها - طرق مكافحتها

لينا جمال





الجرائم الإلكترونية

ماهيتها – طرق مكافحتها

الجرائم الإلكترونية

ماهيتها – طرق مكافحتها

لينا جمال محمد

الطبعة الأولى

2016م





المملكة الأردنية الهاشمية

ررقم الأيداع لدى دائرة المكتبة الوطنية

(2016/4/1437)

محمد، لينا جمال

الجرائم الإلكترونية/ لينا جمال محمد.- عمان : دار خالد اللحياني للنشر والتوزيع ، 2016

( ) ص.

ر.إ .: 1437/4 /2016





دار خالد اللحياني للنشر والتوزيع

المملكة العربية السعودية – مكة المكرمة

ص. ب 21402

الرمز البريدي 21955

هاتف: 00966555008626

البريد الإلكتروني: shs1427@gmail.com

دار من المحيط إلى الخليج للنشر والتوزيع

هاتف:

00962799817307

00966506744232

البريد الإلكتروني

azkhamis01@homail.com

azkhamis01@yahoo.com

المقدمة

تعد الجرائم الإكترونية من الجرائم الحديثة التي تُستخدم فيها شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها، وجرائم الإنترنت كثيرة ومتنوعة ويصعب حصرها ولكنها بصفة عامة تشمل الجرائم الجنسية، وجرائم ترويج المخدرات، وتعليم الإجرام أو إرهاب كصنع المتفجرات، إضافة إلى جرائم الفيروسات واقتحام المواقع، إضافة إلى جرائم سرقة المعلومات أو حتى البيانات الشخصية، وتتعدى ذلك لتشمل تحويل الأرصدة في البنوك عبر الشبكة، وتكمن خطورة هذا النوع من الجرائم في أنها لا تعرف الحدود والمكان، ولا توجد لها أدلة مادية تدل عليها أو على من يرتكبها' ونحن في عصر التكنلوجيا أصبحنا نستخدم الإنترنت في كافة جوانب الحياة من اتصالات ومعاملات مالية وتعليم...إلخ، ما أدى إلى زيادة في نسبة وقوعنا في فخ الجريمة الإلكتروني، من هذا المنطلق يسعى هذا الكتاب إلى رفع الوعي لدى أبنائنا وبناتنا بأهمية أخلاقيات التعامل مع الإنترنت، وإكسابهم المعلومات والمهارات اللازمة لرفع درجة سلامتهم الشخصية فيما يتعلق بالتعامل مع الرموز السرية والحذر من مخاطر كشف الهوية على الإنترنت والإتصال بالأفراد والهيئات المناسبة لطلب مساعدتهم في مواقف حياتية متنوعة.

الفصل الأول

مدخل إلى

تكنلوجيا المعلومات والإنترنت

علم الحاسوب

تـعريـف الـكـمـبـيوتـر:

حاسوب أو حاسب، أو كمبيوتر، هو جهاز يقوم بمعالجة المعلومات وفق إجراء محدد. تعود التسمية باللغة العربية إلى الجذر حَسَبَ الذي يستعمل في الكلمات التي لها علاقة بإجراء العمليات على الأرقام. وكلمة "حاسوب" هي صيغة أسم الآلة من هذا الجذر. يتكون الحاسوب من عتاد وبرمجيات يقومان معا في تأدية وظيفة محددة.

مـكـونـات الـحـاسـوب :

يقصد بمكونات الحاسوب المكونات الصلبة او العتاد Hardware فقط. من الممكن القول أن أي نظام حاسوبي يحتوي على الأجزاء التالية بأشكاله المختلفة:

وحدة المعالجة المركزية CPU لمعالجة العمليات الحسابية و تنفيذها

اللوحة الأم MotherBoard

ذاكرة memory Random Access RAM

وحدة إدخال وإخراج البيانات مثل لوحة المفاتيح والفأرة والشاشة.

وهناك مكونات أخرى تعتبر مكملة لعمل الحاسوب مثل:

الطابعة

الماسح الضوئي

الأجهزة الصوتية و المرئية أو الوسائط المتعددة

بالإضافة إلى المكونات الصلبة فإن الحاسوب يحتاج إلى:

نظام تشغيل ليس من مكونات الحاسوب تعتبر من المكملات

برامج ليس من مكونات الحاسوب تعتبر من المكملات

أنـــواع الـحـــواســيــب:

يمكن تقسيم الحواسيب إلى:

حواسيب الإطار الرئيسي: وهي الحواسيب ذات السعات التخزينية الضخمة والكفاءة العالية في المعالجة والتي تستخدم في المنشآت الكبيرة كالدوائر الحكومية والجامعات والشركات الكبرى، حيث يتم ربط الجهاز الرئيسي بمجموعة من الأجهزة الفرعية تسمى نهايات طرفية.

حواسيب شخصية: وهي الحواسيب التي نراها في المنازل والمكاتب. ويستعمل مصطلح الحاسوب أو كمبيوتر بشكل عام في الإشارة إلى الحواسيب الشخصية.

<u>حواسيب كفية:</u> وهي أجهزة صغيرة لا يتجاوز حجمها كف اليد، تستخدم في إجراء بعض المهام الحاسوبية البسيطة كحفظ البيانات الضرورية والمواعيد، وقد توسع استخدامها مؤخراً حتى أصبحت تضاهي باستخداماتها الحواسيب الأخرى، حيث تستخدم بعضها في الدخول إلى الانترنت أو الاستدلال في الطرق من خلال أنظمة الابحار.

<u>حواسب مدمجة:</u> وهي الحواسيب الموجودة في العديد من الأجهزة الإلكترونية والكهربائية في هذه الأيام. إذ أن العديد من الأجهزة تحتوي حواسيب لأغراض خاصة. فمثلاً توجد الحواسيب في الهواتف السيارات وأجهزة الفيديو والطائرات وغيرها.

<u>عـتـاد الـكـمـبـيـوتـر</u> :

إن الكمبيوتر يتكون من مفاتيح وأسلاك ولوحات دوائر إلكترونية وقطع ورقائق إلكترونية مدمجهChips ، ومحرك قرص التخزين الصلب، ومحرك قرص التخزين المرن، بالإضافة إلى طابعة ولوحة مفاتيح وماوس وشاشة إظهار الصورة (سنتعرض لذلك بالتفصيل لاحقا). كل هذه المكونات متصلة مع بعضها البعض لتكون نظاما له القدرة على القيام بمهمات الحسابات واستيعاب معطيات المعلومات كنوع من هذه المهمات ثم التعامل معها لإعطاء النتائج. أن قدرة الكمبيوتر هذه في تداول ومعالجه المعلومات المختلفة أعطت للكمبيوتر القوة، هذه المعلومات تكون عادة في

غاية الأهمية سواء للأفراد أو للمؤسسات. الاستخدامات العملية للكمبيوتر: كما ذكرنا فإن الكمبيوتر بحد ذاته عبارة عن جهاز إلكتروني يتكون من مجموعة من المعدات الصلبة. وحتى يقوم هذا الجهاز بالعمل الذي تريده، فهو بحاجة إلى برنامج يقوم كواسطة بين تلك المكونات بعضها وذلك حتى تكون فيما بينها وحدة واحدة. وكذلك تكون واسطة بين تلك الوحدة والشخص الذي يقوم بتشغيل الكمبيوتر. إن هذا البرنامج هو برنامج التشغيل والذي من أشهرها برنامج ويندوز المعروف. تحتوي معظم برامج التشغيل أيضا على إمكانيات تجعل باستطاعتنا القيام ببعض الأعمال التطبيقية البسيطة الخاصة بالكتابة والرسم وبعض الألعاب وغيرها. وهذه الأعمال في الواقع ليست هي التي يطمح إليها مستخدم الكمبيوتر، ولذلك نلجأ إلى استخدام البرامج التطبيقية التي تقوم بعمل أو أعمال محددة في أحد الجوانب المهمة المفيدة للإنسان .

نــبــذة تــاريــخــيــة عــن الــكــمــبــيــوتــر:

كان أول تقديم للكمبيوتر منذ أكثر من خمسين عاما، وبالتحديد سنة 1946 حيث كان يتكون من أكثر من 18000 صمام إلكتروني، وهذه الصمامات هي نوع معقد بعض الشيء من الأدوات الإلكترونية التي لها شكل مصباح الإضاءة الكهربي المعروف وذو الحجم المتوسط. وهي مماثلة للصمامات التي كانت تستعمل لتشغيل الراديو لمدة طويلة من الزمن وحتى اختراع الترانزيستور، وكذلك لتشغيل التلفزيون في بداية عهده. كان الكمبيوتر في

حينها يحتل بناية كاملة، ويزيد وزنه عن ثلاثين طنا. وهذا يعني أن وزنه أكثر من وزن ثلاثين سيارة. وكانت تلك البناية في حاجة لأجهزة تبريد عملاقة لإزالة الحرارة الناجمة عن تلك الصمامات الإلكترونية. ومع ذلك فإن فعاليته لم تكن أكثر من فعالية آله حاسبة جيب صغيرة مما يستعملها تلاميذ المدارس الآن !!

أجيال الكمبيوتر:

الجيل الأول :

بدأ في الخمسينات.

إنتاج حاسوب UNIVAC.

استخدمت حواسيب هذا الجيل الصمامات المفرغة، وكانت هذه الصمامات تحتاج إلى حرارة عالية، لذلك فقد كانت تستهلك طاقة كهربائية عالية. كان حجم هذه الحواسيب كبيراً جدا، ووزنها ثقيل و سرعة تنفيذ العمليات بطيئة إلى حد ما (20 ألف عملية في الثانية).

اعتمدت على لغة الآلة (التي تعتمد على النظام الثنائي) في كتابة البرامج، وبالتالي كانت البرامج معقدة و استخدمت الاسطوانة المغناطيسية كوسيط لإدخال البيانات، وآلات طباعة بدائية لاستخراج النتائج.

الجيل الثاني :

بدأ من 1959 إلى 1965.

استبدلت الصمامات المفرغة بالترانزستور حيث كان أصغر حجما وأطول عمرا ولا يحتاج طاقة كهربائية عالية.

كان حجم حواسيب هذا الجيل أصغر من الجيل الأول و أصبح أكثر سرعة في تنفيذ العمليات حيث بلغ سرعته مئات الآلاف في الثانية الواحدة.

استخدمت الأشرطة الممغنطة كذاكرة مساندة، واستخدمت الأقراص المغناطيسية الصلبة.

استخدمت بعض اللغات الراقية مثل Fortran , Cobol.

الجيل الثالث :

1970-1965

إنتاج الدوائر المتكاملة والمصنوعة من رقائق السيليكون.

أصبحت أصغر حجما بكثير وانخفضت تكلفة إنتاج الحواسيب.

تم إنتاج سلسلة حاسبات.IBM 360

أصبحت سرعة الحواسيب تقاس بالنانوثانية.

تم إنتاج الشاشات الملونة وأجهزة القراءة الضوئية.

تم إنتاج أجهزة إدخال وإخراج سريعة.

ظهرت الحواسيب المتوسطة mini computer system والتي تشترك مجموعة طرفيات بجهاز حاسوب مركزي.

الجيل الرابع :

1980-1970

حصلت ثورة كبيرة على معدات الحاسوب وعلى البرمجيات في نفس الوقت.

استخدمت الدوائر المتكاملة الكبيرة LSI

تميزت حواسيب هذا الجيل بصغر الحجم وزيادة السرعة والدقة و الوثوقية وسعة الذاكرة وقلة التكلفة.

أصبحت السرعة تقاس بملايين العمليات في الثانية الواحدة.

ظهرت الذاكرة العشوائية RAM والذاكرة الدائمة ROM أصبحت أجهزة الإدخال والإخراج أكثر تطورا وأسهل استخداما.

طورت نظم التشغيل، مما أدى إلى ظهور الحاسبات الشخصية.

ظهرت لغات ذات المستوى الراقي والراقي جدا.

ظهرت الأقراص الصلبة المصغرة والأقراص المرنة والراسمات.

الجيل الخامس :

توفر حاسبات هذا الجيل زيادة في الإنتاجية حيث سيتعامل معها الإنسان مباشرة لأن بإمكانها فهم المدخلات المحكية، المكتوبة والمرسومة.

زيادة هائلة في السرعات وسعات التخزين.

ظهور الذكاء الاصطناعي ولغات متطورة جدا.

حواسيب عملاقة ذات قدرات كبيرة جدا، وتمتاز بدرجة عالية جدا من الدقة.

إيجابيات وسلبيات الحاسب الآلي في علم الجريمة

للحاسب الآلي وللأنظمة على مختلف مظهرها بما في ذلك شبكة الاتصالات الدولية (الإنترنت) وشبكة المعلومات العالمية (web) ، والبريد الإلكتروني أو الرقمي (E-mail) ، والمجاميع الإخبارية (New Groups)[1]، ومواقع نقل الملفات (File Transferee Protocol) وغرف المحادثة (Chatting Rooms)....الخ ؛ مزايا في مجال الإعلام والاتصالات والتراسل وإجراء المكالمات الهاتفية الدولية والاتصالات البريدية بأسعار

[1] - وهي عبارة عن مساحات تغطي موضوعات علمية وثقافية وفنية وتاريخية ، وكل ما يتعلق بالاهتمامات الإنسانية الأخرى .

زهيدة، وكذلك إجـراء الحوار الذي من خلاله ظهرت حالات التعارف والاتفـاق عـلى الـزواج وبصورة رسمت شكلاً جديداً للعلاقات الإنسانية تعتمد على التفاهم والتفكـير المـشترك، كـما لهذه الأنظمة مزايا أخر في مجال التعليم والبحث العلمي، وأحدث ما توصل إليه العلـم ومـا استجد في العلوم المختلفة ، وكذلك تتبع أخبار العالم كـما تراهـا وكـالات الأنبـاء ومحطـات الأخبار العالمية والصحف، و أخبار البورصة.

وفي مجال الملاحقة الجنائية لهذه النظم مزايا في تقديم الخدمات منها :

1- تسهيل القبض على المجرمين :

يستخدم الحاسب الآلي في مكافحة الجرائم والكشف عتها والتعرف على مرتكبيها بالصوت والصورة بل وببصمة الصوت والعين التي تفشل محاولة المجرمين في خداع الحاسب الآلي بتغيير ملامحهم عن طريق إجراء عمليات جراحية أو غيرها، كما استخدم الحاسب الآلي أيضا في بعض بلدان أوروبا في عرض صور المطلوب القبض عليهم عوضا عن النشر في الصحف وشاشات التلفاز لحث الجمهور على الإبلاغ عنهم عن طريق الاتصال بالبوليس الدولي (الإنتربول).

2- التنبؤ بالجرائم :

من خلال دراسة الأبعاد السكانية والاقتصادية واتجاهات وسلوكيات السكان وغيرها من النواحي الأخرى على الشبكة يمكن التنبؤ بمعدلات

الجرائم وأنواعها، وقد ثبت من خلال الإحصائيات العالمية أن معدلات الجرائم وحالات الانتحار في أمريكا وأوروبا قد انخفضت بعد اتساع قاعدة المشتركين في شبكة الإنترنت[2] .

3- نظام المراقبة الإلكترونية :

المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية قصيرة المدة خارج السجن، وذلك بإلزام المحكوم عليه بالمكوث في مقر إقامته أو في أي مقر آخر يحدده خلال ساعات معينة يحددها القاضي، وللمحكوم عليه الالتحاق بعمله أو الاستمرار في دراسته، وكذلك الوفاء بمتطلباته الأسرية كافة وغيرها ؛ ويتم تطبيق هذا النظام من خلال استخدام التكنولوجيا الحديثة، حيث تعهد هذه المهمة في مراقبة المحكوم عليه إلى جهاز إرسال يوضع على يدّ المحكوم عليه يمكّن مؤسسة الإصلاح والتأهيل (المؤسسة العقابية) من التأكد من تنفيذ العقوبة[3]..

[2] - د. جميل عبد الباقي الصغير ، الانترنت و القانون الجنائي ، دار النهضة العربية ، القاهرة ، 2001 ، ص13 وما بعدها.

[3] - د.عمر سالم ، المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، دار النهضة العربية ، الطبعة الأولى ، القاهرة ، 2000 ، ص 10 .

سلبيات الحاسب الآلي وموقف التشريعات من الجرائم الإلكترونية

بعد تطور أشكال الجريمة مع استخدام الحاسب الآلي والانترنت واستهدافها لكافة المصالح و الحقوق ، أصبحت الجرائم الإلكترونية تقع على الأشخاص و الأموال والمعلومات ، سواء في القتل أو التحريض على الانتحار و التسبب في الأضرار والمضايقات غير الأخلاقية ، و انتهاك سرية البيانات الشخصية ، و تحريض القاصرين على أنشطة جنسية غير مشروعة ، و التحرش الجنسي بالقاصرين ، و نشر الأشياء الفاضحة المخلة بالحياء و تخريب النظم و المعلومات وخلق البرامج الضارة وإرسالها و إدخال معلومات خاطئة إلي نظام الحاسب الآلي والاحتيال و التلاعب في البطاقات المالية وسرقة المعلومات و تزوير البريد الإلكتروني وتشجيع مشروعات المقامرة وترويج المواد الكحولية و المخدرات وتعطيل الأعمال الحكومية و العبث بالأدلة القضائية وتهديد السلامة ، ونشر الإرهاب الإلكتروني وغيرها من الممارسات غير المشروعة التي ترتكب بواسطة الحاسب الآلي و الانترنت .

شبكات الحاسب الآلي

يمكن تعريف شبكة الحاسب الآلي بأنها مجموعة من أجهزة الحاسب و الأجهزة المحيطة (peripherals) تتصل ببعضها البعض وفق نظام اتصال معين يسمح للمستخدمين التشارك في استخدام الموارد (

Resources) مثل الطابعات،و الموديم، ومحركات الأقراص، وغيرها. فيمكن تلخيص فوائد استخدام شبكات الحاسب الآلي في النقاط التالية: ـ

المشاركة في الموارد: Resources Sharing ـ

تؤمن شبكات الحاسب إمكانية تارك المستثمرين في موارد الشبكة المختلفة مثل الطابعات و الماسحات الضوئية و الملفات و غيرها من موارد الشبكة المختلفة.

تبادل المعلومات: Information Exchange ـ

تبادل المعلومات و الملفات الخاصة بالتطبيقات على خطوط الشبكة في وقت سريع بتكاليف منخفضة و بدرجة كبيرة من الأمان.

إمكانية الاتصال عن بعد:Telecommunicating ـ

أصبح بالإمكان الاتصال بين مستخدمي الشبكة عن طريق:

الاتصال على الخط المباشر.Online

استخدام خدمة البريد الإلكتروني Electronic mail لتبادل الرسائل.

التخاطب عبر برامج الاتصال.Chatting

التشارك في البرمجيات: sharing the software

تؤمن شكبة الحاسبات إمكانية تشارك المستثمرين للبرمجيات و الأنظمة المتواجدة على أجهزة الشبكة.

مصطلحات متعلقة بالشبكة :-

الخادم Server: أجهزة حاسب فائقة القدرة على التخزين وذو قدرات معالجة كبيرة يقوم بتزويد الشبكة بالموارد و الخدمات، وهو أهم اجهزة الشبكة.

العميل Client: أجهزة حاسبات شخصية أو وحدات طرفية يحصل على الموارد و الخدمات من قبل الخادم، وليس له أي صلاحيات بالتحكم

مصادر الشبكة Resource : عبارة عن الملفات والطابعات و الأجهزة المستخدمة.

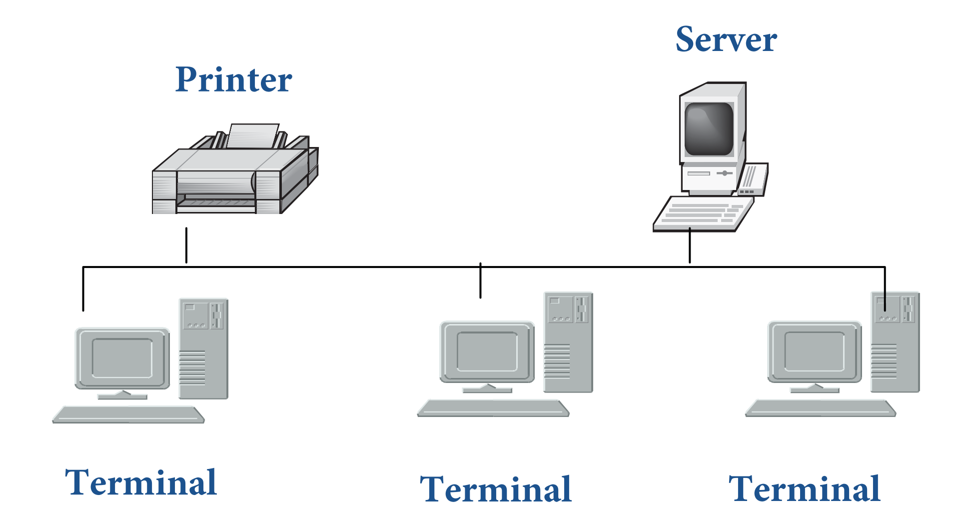
أنواع الشبكات حسب البعد :-

يمكن تقسيم الشبكات على حسب البعد إلى ثلاثة أنواع أساسيه وهي:-

شبكات محلية Local Area Network ((LAN) :-

في بداية ظهور الشبكات كانت تتكون من عدد قليل من الأجهزة ربما لا يتجاوز العشرة متصلة مع بعض، هذا النوع من التشبيك أصبح يعرف بLocal Area Network = LAN ومتصل معها جهاز طباعة وهذه الأجهزة تعمل مع بعضها ومتصلة مع بعضها البعض في مساحه جغرافية

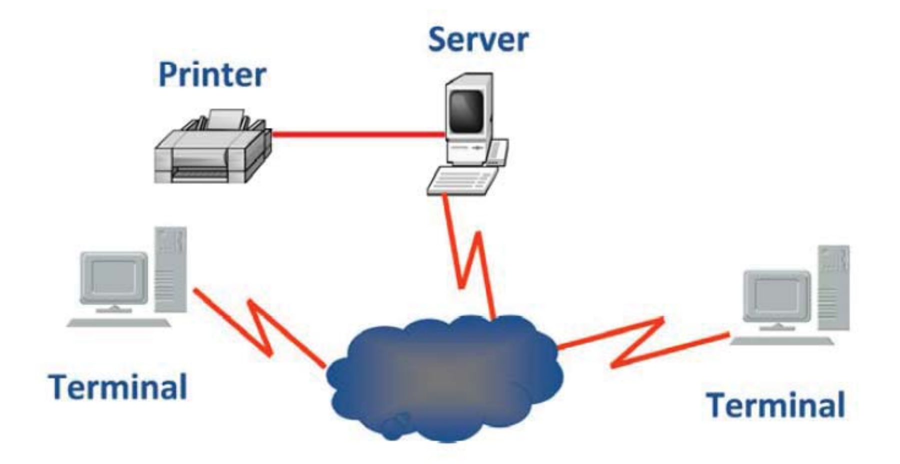
صغيره كأن تكون داخل مكتب أو مجموعه مكاتب في بناية واحده أي أنها تعمل ضمن مساحه محدودة وتتميز هذه الشبكة عن غيرها بسرعه كبيره في تبادل الملفات والاستفادة الفورية من كوارد الشبكة.



ب. شبكات واسعه Wide Area Network (WAN):-

في بداية ظهور الشركات الكبيرة لم تتمكن شبكة LAN من دعم احتياجات هذه الشركات وربطها مع بعضها لهذا كانت الحاجه إلى ظهور الشبكة الواسعة.

(هنا يتم ربط الأجهزة في مناطق مختلفة (مباني متباعدة) و ذلك باستخدام وسائط مثل: خط الهاتف أو القمر الصناعي.)



جـ شبكة الإنترنت (the Internet) :-

الإنترنت: هي عبارة عن شبكة عالمية تربط بين مختلف شبكات الكمبيوتر على النطاق المحلي والعالمي لجعلها منظومة متكاملة، تساعد المستخدم على التنقل في شعاب هذه المنظومة العالمية المعقدة عبر خطوط الهاتف والأقمار الصناعية وأجهزة الحاسب الآلي. وهي اختصار لعبارة International Network

(سوف نتعرض لها لاحقاً)

أنواع الشبكات حسب المكونات:-

1. Peer to Peer Networks (شبكة النظير):-

بحيث يكون كل جهاز هو(عميل/ وخادم) في نفس الوقت

المميزات :

سهلة التثبيت

توفير وظيفة مراقب

مقدرة المستخدمين على السيطرة على

مصادر الشبكة

قلة التكلفة

عدد المستخدمين محدود

العيوب :

قلة المستخدمين

لا يوجد نظام تخزين مركزي

الحماية ضعيفة



Server Based Network.2 (شبكة الخادم):-

بحيث يكون هناك نوعين من الاجهزه احدها هو المسؤول (الخادم) والاجهزه الاخرى هي عميل

المميزات:

حماية مركزية قوية

التخزين المركزي

مقدرة الخادم المشاركة في

الأجهزة و البرامج

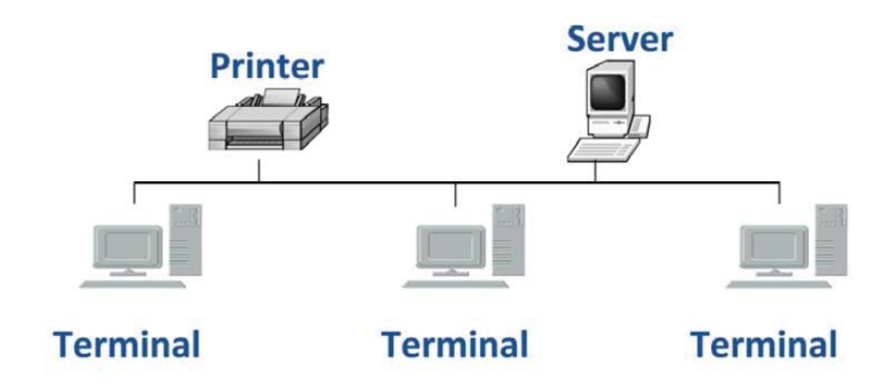
سهولة إدارة الأعداد الكبيرة

من المستخدمين

العيوب:

الأجهزة و نظام التشغيل غالية الثمن

تحتاج مراقب شبكة



شبكة الإنترنت:-

تعريف الإنترنت وبداياته واستخداماته :

"الإنترنت هو جزء من ثورة الاتصالات ويعرف البعض الإنترنت بشبكة الشبكات في حين يعرفها البعض الآخر بأنها شبكة طرق المواصلات السريعة، ويمكن تعريف الإنترنت بشبكة الشبكات"

بداية الإنترنت: بدأ الإنترنت في 1969/1/2 عندما شكلت وزارة الدفاع الأمريكية فريقا من العلماء للقيام بمشروع بحثي عن تشبيك الحاسبات وركّزت التجارب علي تجزئة الرسالة المراد بعثها إلى موقع معين في الشبكة ومن ثم نقل هذه الأجزاء بشكل وطرق مستقلة حتى تصل مجّمعة إلى هدفها وكان هذا الأمر يمثل أهمية قصوى لأمريكا وقت الحرب ففي حالة نجاح العدو في تدمير بعض خطوط الاتصال في منطقة معينة فان الأجزاء الصغيرة

يمكن أن تواصل سيرها من تلقاء نفسها عن أي طريق آخر بديل إلى خط النهاية. ومن ثم تطور المشروع وتحول إلى الاستعمال السلمي حيث انقسم عام 1983 إلى شبكتين احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) كما احتفظت بغرضها الأساسي وهو خدمة الاستخدامات العسكرية. وسميت الشبكة الثانية باسم (MILNET) للاستخدامات المدنية أي تبادل المعلومات وتوصيل البريد الإلكتروني ومن ثم ظهر المصطلح " الإنترنت " حيث أمكن تبادل المعلومات بين هاتين الشبكتين. وفي عام 1986 أمكن ربط شبكات خمس مراكز للكمبيوترات العملاقة وسميت (NSFNET) والتي أصبحت العمود الفقري وحجر الأساس لنمو وازدهار الإنترنت في أمريكا ومن ثم دول العالم الأخرى.

من يملك الإنترنت؟؟ لا أحد في الوقت الراهن يملك الإنترنت ففي البداية يمكن القول بان الحكومة الأمريكية ممثلة في وزارة الدفاع ثم المؤسسة القومية للعلوم هي المالك الوحيد للشبكة ولكن بعد تطور الشبكة ونموها لم يعد هناك مالك لها واختفي مفهوم التملك ليحل محله ما أصبح يسمي بمجتمع الإنترنت كما أن تمويل الشبكة تحول من القطاع الحكومي إلى القطاع الخاص. ومن هنا ولدت العديد من الشبكات الإقليمية ذات الصبغة التجارية حيث يمكن الاستفادة من خدماتها مقابل اشتراك. (أبو الحجاج 1998م).

توسع الشبكة: في عام 1985م كان هناك اقل من ألفي حاسوب آلي مرتبط بالشبكة وفي عام 1995م وصل العدد إلى (5) مليون حاسوب وفي

عام1997م تتجاوز حاجز الـ (6) مليون وتستخدم ما يزيد علي (300) ألف خادم (SERVER) أي شبكة فرعية متناثرة في أرجاء العالم,ويمكن القول بان عدد المستخدمين الجدد يبلغ (2) مليون شهريا أي ما يعني انضمام (46) مستخدم جديد للشبكة في كل دقيقة (السيد، 1997 م).

بروتوكولات الإنترنت :

حتى تستطيع إقامة اتصال بين الحاسوبات المختلفة فان الأمر يتطلب وجود مجموعة من القواعد المتفق عليها والمعروفة باسم البروتوكولات، وقد تنوعت أسماء هذه البروتوكولات بين الأسماء الطريفة مثل جوفر (Gopher) والأسماء الطويلة المزعجة التي تم اختصارها مثل بروتوكول نقل النص المتشعب HTTP)) بدلا من (Hypertext Transfer Protocol) أو بروتوكول التحكم في النقل (TCP/IP) بدلا عن مسماه الطويل (Transmission Control Protocol/Internet Protocol)

فما هي هذه البرتوكولات وما هي وظائفها :

أولا : بروتوكول الإنترنت (IP) (Internet Protocol) أحد أهم البروتوكولات الأساسية والـ (IP) عبارة عن رقم مكون من أربعة أجزاء، يعرّف الجزء الأول من الرقم بدءاً من اليسار المنطقة الجغرافية، والجزء الثاني يحدد المنظمة أو الحاسوب المزود، أما المجموعة الثالثة من الأرقام فتحدد مجموعة الكمبيوترات التي ينتمي إليها الجهاز، والمجموعة الرابعة يحدد الجهاز

المستخدم. ويمكن اعتبار الـ IP)) نوع من الخرائط الخاصة بالانترنت، حيث يمكن الاتصال بأي حاسوب أو بأي موقع من خلال نقطة معينة على هذه الخريطة.

ثانيا : لغة ترميز النص التشعبي وبروتوكول نقل النص التشعبي

Language and HTML Hypertext Markup and hypertext Transfer Protocol (HTTP)

يتحكم HTML)) و (HTTP) معا في الشبكة العنكبوتية (WWW) فـ الـ(HTML) طريقة لإضافة تنسيق إلى ملفات النصوص بحيث يمكنك رؤية أشياء مثل العناوين، والكلمات المراد تحديدها للفت الانتباه، والفقرات التي يتم توسيطها بالصفحة، والصورة المدرجة داخل النص، وذلك عند استخدامك لمستعرض ويب (HTML)أما (HTTP) فهو بروتوكول يقوم بتعريف كيفية إرسال و استقبال ملفات HTML))

ثالثا: بروتوكول التحكم في النقل(Transmission Control Protocol) أو ما يعرف اختصارا بـ(TCP) هو البروتوكول الذي يعرِّف البناء الخاص بالبيانات وكيفية إرسالها بين الحاسوبات،وعادة يتم تقسيم هذه البيانات إلى أجزاء عند إرسالها، ومن ثم يعمد إلى إعادة تجميعها وإعادتها إلى ترتيبها الأصلي عند وصولها إلى نقطة النهاية. ونظرا لاشتراك البروتوكول ((TCP و IP)) فقد جرى العمل عادة إلى الإشارة إليهما مجتمعين بـ (TCP/IP)

رابعا: تلنت (Telnet) : هو بروتوكول يقوم يتيح لك تشغيل جهاز آخر من خلال جهازك. فعندما تستخدم برنامج (Telnet) يمكنك الدخول إلى كمبيوتر آخر وتشغيل برامج كما لو كنت تجلس أمامه.

خامسا: جوفر (Gopher) يتم عرض محتويات الجهاز الخادم الذي يستخدم بروتوكول (Gopher) على هيئة قوائم فرعية ويمكنك اختيار أي عنصر من عناصر هذه القوائم. وما يميز هذا البروتوكول هو إعطاء المستخدم إمكانية اختيار أي عنصر من عناصر هذه القوائم ولو كانت على خادم (Gopher) آخر يختلف عن الخادم الذي قدم لك القائمة الأولى.

سادسا : بروتوكول نقل أخبار الشبكة:

(Network News Transfer Protocol) والمعروف اختصارا بـ NNTP تقوم أجهزة الخادم الخاصة بـيوزنت (UseNet) بتخزين الرسائل وتبادلها باستخدام بروتوكول (NNTP) وبهذه الطريقة يستطيع العديد من الأفراد قراءة و إرسال الرسائل إلى هذه الأجهزة الخادمة باستخدام برنامج لقراءة الأخبار.

مستلزمات الاتصال بالشبكة:

حاسب إلى 2- مودم 3- الاشتراك في الخدمة 4- برامج تصفح الشبكة

خدمات الإنترنت:

1- البريد الإلكتروني :لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص له عنوان بريدي بصورة سريعة جدا لا تتعدى دقائق.

2- قوائم العناوين البريدية : تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعات من الأشخاص لهم اهتمامات مشتركة.

3- خدمة المجموعات الإخبارية: تشبه خدمة القوائم البريدية باختلاف أن كل عضو يستطيع التحكم في نوع المقالات التي يريد استلامها.

4- خدمة الاستعلام الشخصي : يمكن الاستعلام عن العنوان البريدي لأي شخص أو هيئة تستخدم الإنترنت والمسجلين لديها.

5- خدمة المحادثات الشخصية : يمكن التحدث مع طرف آخر صوتا وصورة وكتابة.

6- خدمة الدردشة الجماعية : تشبه الخدمة السابقة إلا انه يمكن التحدث مع أكثر من شخص في نفس الوقت حيث يمكن تنظيم مؤتمر لعدد من الأفراد.

7- خدمة تحويل أو نقل الملفات : لنقل الملفات من حاسب إلى آخر FTP وهي اختصار (FILE TRANSFER PROTOCOL).

8- خدمة الأرشيف الإلكتروني :ARCHIE)) يمكن البحث عن ملفات معينة قد تكون مفقودة في برامجك المستخدمة في حاسبك.

9- خدمة شبكة الاستعلامات الشاملة : GOPHER)) يسمح للمستخدم بتشغيل والاستفادة من خدمات الكثير من الموارد الأخرى مثل خدمة نقل الملفات وخدمة المشاركة في قوائم العناوين البريدية حيث يفهرس المعلومات الموجودة علي الشبكة

10- خدمة الاستعلامات واسعة النطاق : (WAIS) تسمي هذه الخدمة باسم حاسباتها الخادمة نفسها وهي أكثر ذكاء ودقة وفاعلية من الأنظمة الأخرى حيث تبحث داخل الوثائق أو المستندات ذاتها عن بعض الكلمات المحورية أو الدالة التي يحددها المستخدم ثم تقدم نتائج البحث في شكل قائمة بأسماء المواقع التي تحتوي علي المعلومات المطلوبة.

11- خدمة الدخول عن بعد : TELNET تسمح باستخدام برامج وتطبيقات في الحاسب الآلي الآخر.

12- الصفحة الإعلامية العالمية : (WORLD WIDE WEB) (WWW) وتسمي أيضا الويب (WEB) : تجمع معا كافة الموارد المتعددة التي تحتوي عليها الإنترنت للبحث عن كل ما تريد في الشبكات المختلفة وإحضارها بالنص والصوت والصورة و الويب نظاما فرعيا من الإنترنت لكنها النظام الأعظم من الأنظمة الأخرى فهي النظام الشامل باستخدام الوسائط المتعددة

برامج التصفح المتوفرة :

هناك العديد من برامج تصفح الانترنت، أهمها:

1- NETSCAPE

2- INTERNET EXPLORER

3- MOSAIC

الفيروسات:

الفيروسات الحاسب آلية هي إحدى أنواع البرامج الحاسب الآلية، إلاّ أنّ الأوامر المكتوبة في هذه البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما، أو حتى مجرد فتح البرنامج الحامل للفيروس، أو الرسالة البريدية المرسل معها الفيروس، إصابة الجهاز به ومن ثَمّ قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به. وقد عرّفها أحد خبراء الفيروسات (Fred Cohen) بأنّها نوع من البرامج التي تؤثّر في البرامج الأخرى، بحيث تعدّل في تلك البرامج لتصبح نسخة منها، وهذا يعنى ببساطة أنّ الفيروس ينسخ نفسه من حاسب آلي إلى حاسب آلي آخر، بحيث يتكاثر بأعداد كبيرة (1999Highley,).

ويمكن تقسيم الفيروسات إلى خمسة أنواع :

الأول: فيروسات الجزء التشغيلي للاسطوانة كفيروس Brain)) و(Newzeland).

الثاني: الفيروسات المتطفلة كفيروس (Cascade) وفيروس (Vienna).

الثالث: الفيروسات المتعددة الأنواع كفيروس (Spanish-Telecom) وفيروس (Flip).

الرابع: الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوس أو الوندوز.

الخامس: يعرف بحصان طروادة، وهذا النوع يصنّفه البعض كنوع مستقّل بحد ذاته، إلاّ أنّه أدرج في هذا التقسيم كأحد أنواع الفيروسات، وينسب هذا النوع إلى الحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاء سلمي إلا أنّ أثره التدميري خطير.

وتعمل الفيروسات على إخفاء نفسها عن البرامج المضادة للفيروسات باستخدام طرق تشفير لتغيّر أشكالها، لذلك وجب تحديث برامج مكافحة الفيروسات بصفة دائمة (عيد،1419هـ : 63-66).

ويختلف الخبراء في تقسيمهم للفيروسات، فمنهم من يقسمّها على أساس المكان المستهدف بالإصابة داخل جهاز الكمبيوتر، ويرون أنّ هناك ثلاثة أنواع رئيسة من الفيروسات هي: فيروسات قطاع الإقلاع(Boot Sector)

وفيروسات الملفات(File Injectors)وفيروسات الماكرو (macro Virus).

وهناك من يقسّمها إلى: فيروسات الإصابة المباشرة (Direct action) وهي التي تقوم بتنفيذ مهمتها التخريبية فور تنشيطها، أو المقيمة (staying) وهي التي تظل كامنة في ذاكرة الكمبيوتر وتنشط بمجرد أن يقوم المستخدم بتنفيذ أمر ما، ومعظم الفيروسات المعروفة تندرج تحت هذا التقسيم، وهناك أيضاً الفيروسات المتغّيرة (Polymorphs) التي تقوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلّل برامج مكافحة الفيروسات.

ومن الجرائم المتعلقة بإرسال فيروسات حاسوبية قيام شخص أمريكي يدعى (Robert Morris) بإرسال دودة حاسوبية بتاريخ الثاني من نوفمبر عام (1988م) عبر الإنترنت، وقد كرّر الفيروس نفسه عبر الشبكة بسرعة فاقت توقع مصمم الفيروس وأدى ذلك إلى تعطيل ما يقارب من (6200) ستة آلاف ومائتي حاسبٍ آلي مرتبط بالإنترنت، وقد قدرّت الأضرار التي لحقت بتلك الأجهزة بمئات الملايين من الدولارات. ولو قُدّر لمصمم الفيروس تصميمه بحيث يكون أشدّ ضرراً، للحقت أضرار أخرى لا يمكن حصرها بتلك الأجهزة، وقد حُكم على المذكور بالسجن ثلاث سنوات بالرغم من دفاع المذكور عن نفسه أنّه لم يكن يقصد إحداث مثل تلك الأضرار(1998Morningstar,).

كيف يتم اقتحام الجهاز؟

لتتم عملية الاقتحام يجب زرع حصان طروادة في جهاز الضحية بعدة طرق منها:

1. يرسل عن طريق البريد الإلكتروني باعتباره ملفاً ملحقاً حيث يقوم الشخص باستقباله وتشغيله، وقد لا يرسل وحده حيث من الممكن أن يكون ضمن برامج، أو ملفات أخرى.

2. عند استخدام برنامج المحادثة الشهير (ICQ).

3.عـند تحميل بـرنامج من أحد المواقع غير الموثوق بها وهي كثيرة جدا.

4.طريقة أخرى لتحميله، تتلخّص في مجرد كتابة كوده على الجهاز نفسه في دقائق قليلة.

5.في حالة اتصال الجهاز بشبكة داخـلية أو شبكة إنترانت.

6.يمكن نقل الملف أيضاً بواسطة برامج (FTP) أو (Telnet) الخاصة بنقل الملفات.

7.كما يمكن الإصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكرو الموجود في برامج معالجة النصوص (2000Nanoart,).

وبصفة عامة فإن برامج القرصنة تعتمد كلياً على بروتوكول الـ ((TCP/IP وهناك أدوات (ActiveX) مصمّمه ومجهّزة لخدمة التعامل بهذا البروتوكول، ومن أشهرها (WINSOCK.OCX) لمبرمجي لغات البرمجة الداعمة للتعامل مع هذه الأدوات. ويحتاج الأمر إلى برنامجين، خادم في جهاز الضحية، وعميل في جهاز المتسلل، فيقوم الخادم بفتح منفذ محدد مسبقاً في جهاز الضحية، في حين يكون برنامج الخادم في حالة انتظار لحظة محاولة دخول المخترق لجهاز الضحية، حيث يتعرف برنامج الخادم (server) على إشارات البرنامج المخترق، ويتم الاتصال، ومن ثَمّ يتمّ عرض كامل محتويات جهاز الضحية عند المخترق، حيث يتمكّن من العبث بها أو الاستيلاء على ما يريد منها.

فالمنافذ (Ports) يمكن وصفها ببوابات للجهاز، وهناك ما يقارب الـ(65.000) منفذ تقريباً في كل جهاز، يميّز كلّ منفذ عن الآخر برقم خاص ولكلّ منها غرض محدد، فمثلاً المنفذ (8080) يخصص أحياناً لمزود الخدمة، وهذه المنافذ غير مادية مثل منفذ الطابعة، وتعدّ جزءاً من الذاكرة، لها عنوان معين يتعرف عليها الجهاز بأنّها منطقة إرسال واستقبال البيانات، وكلّ ما يقوم به المتسلل هو فتح أحد هذه المنافذ للوصول لجهاز الضحية وهو ما يسمى بطريقة الزبون/الخادم Client\Server)) حيث يتمّ إرسال ملف لجهاز الضحية، يفتح المنافذ فيصبح جهاز الضحية (server)، وجهاز المتسلل

(Client)، ومن ثَمّ يقوم المتسلل بالوصول لهذه المنافذ باستخدام برامج كثيرة متخصصة كبرنامج ((Net Bus أو ((Net Sphere.

البحث في الإنترنت

تحتوي إنترنت، وشبكة (ويب) على وجه الخصوص حالياً على ملايين الصفحات من المعلومات معظمها على شكل نصوص. وتنمو كتلة النصوص التي تحتوي عليها إنترنت بمعدلات متسارعة فضلاً عن خضوعها لعمليات التحديث المستمرة على مدار اليوم بل الساعة. ويطرح كل ذلك تحدياً جديداً أمام أولئك الذين يبحثون عما يحتاجونه من معلومات في هذا البحر الزاخر بالمعلومات.

غير أن مشكلة البحث عن المعلومات في النصوص لم تنشأ مع ظهور إنترنت، بل تعود جذورها إلى عهد الكتب المطبوعة، ولتسهيل عملية البحث عن موضوع معين في كتاب مطبوع، تضم الكتب الحديثة في صفحاتها الأخيرة فهرساً للكلمات الدليلية الهامة (الكلمات المفتاحية) وأمام كل منها أرقام الصفحات التي وردت بها الكلمة. وقد إعتمدت أساليب البحث عن المعلومات بواسطة الكمبيوتر على منهجية مشابهة لمنهجية إستخدام كلمات دليلية (Keywords) كتلك المستخدمة في الكتب التقليدية. وتمتاز الأدلة المستخدمة في نظم إسترجاع المعلومات بإستخدام الحاسب، بإتساع نطاقها مقارنة بأدلة الكتب.

ومشكلات البحث عن المعلومات خلال الإنترنت ناتجة من سببين رئيسيين، السبب الأول هو كثرة المعلومات الموجودة على الشبكة، فهناك ملايين صفحات الوب المتشابكة وكذلك مواقع الجوفر (Gopher) ومواقع (FTP) بالإضافة إلى الملايين من مجموعات الأخبار (News-Group) وقوائم البريد (Mailing Lists). السبب الثاني هو عدم وجود هيئة أو منظمة موحدة تشرف على تنظيم هذه المعلومات، بمعنى أنه لا يوجد كتالوج مركزي لهذه الموارد المتاحة ولا يوجد مكان واحد موحد يمكنك الذهاب إليه للبحث عما يريد.

ومع اتساع قاعدة النصوص. كما هو الحال مع شبكة إنترنت، تصبح عملية إسترجاع المعلومات بإستخدام دليل الكلمات غير عملية وتؤدي هذه الطريقة إلى إسترجاع أعداد كبيرة من النصوص التي تحتوي على الكلمات الدليلية التي تبحث عنها، بالإضافة إلى أن هذه النصوص قد لا يكون لمعظمها صلة وثيقة بالموضوع قيد البحث على الرغم من إحتوائها على الكلمة المطلوبة على سبيل المثال إذا كنت تبحث عن معلومات عن تاريخ بعض الدول وأدخلت أسم الصين.

2- أهم المواقع التي تقدم خدمات البحث في شركة إنترنت

1. اكسيت (Excite)

تقدم هذه الخدمة شركة (Architext Software) وقد تم تقديمها على الشبكة منذ وقت قصير. وتشمل هذه الخدمة أداتين ةتتيح البحث عن مواقع معينة على شبكة ويب (Wib) الأولى : البحث في الشبكة (Network) والبحث في المجموعات الاخبارية (Newsgroups) الخاصة بشبكة (Usenet). ويمكن استخدام كلمات مفتاحية في عملية البحث أو إستخدام مفاهيم كمنطلق للبحث مع إمكانية تحديد نطاق للبحث. أما الأداة الثانية فهي مراجعة الشبكة (Netreviews) وهي توفر مخططا هرميا لمحتويات شبكة ويب مبوبة حسب الموضوعات وتفرعاتها.

ويتم تحديث قاعدة البيانات الخاصة باكسيت اسبوعيا وهي تضم حالي 105 بليون صفحة ويب و 50000 صفحة أخبار وعنوان هذه الخدمة على شبكة ويب هو : **www.excite.comhttp://**

2.أنفوسيك (Infoseek)

تتوفر هذه الخدمة بشكل مجاني أو مدفوع الأجر. وتغطي الخدمة المجانية شبكة ويب ويوزنت (Usnet). ونتيجة لذلك يتزاحم معظم المستخدمين على هذه الخدمة مما يصعب معه الوصول إليها. وتغطي هذه الخدمة المجانية ما يقرب من مائة عنوان للبحث أما الخدمة المدفوعة الأجر فتغطى ما يقرب من مائتين

عنوان بالإضافة إلى سرعة استجابتها لطلبات البحث. وتقدم " انفوسيك " نتائج عملية البحث في صورة عناوين الموضوعات المرئية بحسب درجة الصلة المتوقعة لموضاعاتها مع مادة البحث.

وعنوان هذه الخدمة على شبكة ويب هو.

http://www.Infoseek.com

3. ليكوسن (Lycos)

وتعتبر هذه الخدمة من أهم وأقوى أدوات البحث في شبكة إنترنت. ولهذه الخدمة دليل للكلمات يضم أكثر من ثمانية ملايين كلمة تغطى أكثر من 90% من محتويات شبكة ويب. ولهذه الخدمة مزايا فريدة تشمل إمكانية البحث عن النصوص والصور والمواد الصوتية والفيدوية وقائمة تضم حوالي 250 من أكثر مواقع شبكة ويب شعبية ويفضل استخدام هذه الشبكة في أعمال البحث المكثفة وليس البسيطة.

عنوان خدمة ليكوس على الشبكة هو :

http:// www.Lycos.cmu.edu

4. ألتا فينستا

تضم هذه الخدمة أكبر فهرس لشبكة ويب وتستطيع من خلالها البحث بين بلايين الكلمات تضمها مايقرب من 21 مليون صفحة ويب وتتيح أيضا

فهرس نص كامل (full text Indox) به أكثر من 13 ألف مجموعة إخبارية (ewsgroups)

5. ماجلان (Magellan)

تقدم خدمة ماجلان دليلا مصنفا لعدد هائل من مواقع شبكة" ويب" وFTP وجوفر Gopher ويوزنت ومجموعات الأخبار ويشمل ذلك تقديم نبذة عن محتويات الموقع ودرجة شعبيته بين مستخدمي شبكة إنترنت ويمكن استعراض محتويات الدليل بمتابعة تفرعات شجرة الموضوعات أو البحث فيها باستخدام كلمات مفتاحية. وتستخدم خدمة ماجلان ضوءا أخضرا للإشارة إلى أن محتويات الموقع تلائم قاعدة عريضة من المستخدمين وخلوه من المواد الاباحية أو النصوص الخارجة.

6. من هنا ؟ How Is Here

تعتبر خدمة من هنا ؟ من أسرع خذدات البحث وأكثرها استخداما بالإضافة إلى أنها خدمة مجانية وتستخدم هذه الخدمة في تحديد مواقع الهيئات والأفراد على الشبكة. كذلك تقدم خدمة من أين ؟ (Who Where ؟) خدمة متميزة للبحث عن أسماء الأشخاص أو الهيئات عن طريق استخدام الحروف الأولى منها.

7. فهرس النص المفتوح (Open Text Indox)

تعتبر هذه الخدمة من أكثر الخدمات شمولاً فلديها امكانية الوصول إلى نحو مليون صفحة في شبكة ويب وتقوم بالبحث خلال 21 مليون كلمة وجملة وتقوم المفهرسات الآلية (Crawlers) بمتابعة آلاف الصفحات يوميا لفهرسة ماتحتويه من كلمات وتقدير " وزن " كل كلمة مقارنة مع الموضوع الرئيسي للنص وعنوان هذه الخدمة هو :

http://www.opentext.com

(Web Crawler) مفهرسات الويب 8 .

تقوم شركة أمريكا أون لاين(America Online) بتوفير هذه الخدمة. لذلك فهي تعتبر خدمة مدفوعة الأجر وليست مجانية. ويستخدم فيها مايشبه أجهزة الروبوت في جمع الكلمات وفهرستها عبر ملايين الصفحات في شبكة ويب " ويب ". وتمتاز هذه الخدمة بسهولة الإستخدام وسرعة الإستجابة لطلبات البحث القائم على المحتوى. كما تحتوي الصفحات الخاصة بهذه الخدمة على معلومات إحصائية هابة عبر شبكة ويب وعنوان هذه الخدمة هو: **www.woberawler.comhttp://**

9. البرمجيات (Shareware)

تقوم هذه الخدمة أسرع وسيلة للحصول على البرمجيات من على الشبكة. ويمكن من خلالها البحث خلال 170,000 ملف وعارضة (Browsing)

بالإضافة إلى إمكانية تحميل هذه البرمجيات(Download) على حاسبك الشخصي باستخدام خدمة FTP للإستفادة منها وعنوان هذه الخدمة هو :

http://www.Shareware.com

10 خادمات الوب (Web Servers Tourist)

يضم هذا الموقع دليلا شاملا للمواقع العلمية والأكاديمية المسجلة لذى الكونسورنيوم ويقوم الذي يتولى الإشراف على شبكة ويب. يضم هذا الدليل دليلا فرعيا من النوع الفهرسي(rectoryWeb Servers Di) مبوبا على أساس جغرافي ودليلا فرعيا آخر على هيئة خريطة للعالم (Virtual Tourist) يمكن التعامل معها بالضغط على مواقع معينة منها بالفأرة. وهذه الخدمة لا توفر آلية للبحث من النوع الذي توفره الخدمات الأخرى.

11. المكتبة الإلكترونية (Electric Library)

يمكن عن طريق إستعراض محتويات هذه المكتبة عدم الحاجة إلى البحث خلال الوب. فهي تضم قاعدة بيانات تحوى ألف صحيفة نصية (ewspaperText N) والعديد من المجلات والدوريات العلمية (Academic Journals) بالإضافة إلى العديد من الصور والمراجع العلمية (Reference Books) والأبحاث والموضوعات الفنية...الخ.

12. آلة البحث العملاقة (Search)

يضم هذا الموقع 250 آلة بحث يتم إستخدامها كآلة بحث عملاقة للغوص خلال أعماق الإنترنت. وتتيح هذه الآلة الولوج إلى كل الخدمات الرئيسية التي تعرضها الشبكة ومئات من قواعد البيانات المتخصصة وعنوان هذه الخدمة هو:**Search.com /www./ http:**

13.الكتالوج العام للإنترنت(Whole Internet Catalog)

يتيح هذا الكتالوج 1600 موقع يمكن الولوج إليها مجانا مع توصيف هذا الموقع بتقديم نبذة عن كل منها والدليل الذي توفره هذه الخدمة منظم بطريقة جيدة ولكنه لا يوفر آلية البحث من النوع الذي توفره الخدمات الأخرى وعنوان هذا الموقع هو :

http://gnn.com /Wic/wics/index.htmI

14 ياهو (Yahoo)

هذا الموقع من أكثر المواقع شعبية على الإنترنت من حيث المترددين عليه. وهذا أول موقع قدم خدمة البحث على الشبكة. لذلك فهو يحتوي على دليل منظم بطريقة جيدة ويضم كل محتويات شبكة ويب بحسب الموضوعات. ويمكن الولوج إلى هذه المحتويات بمتابعة إرشادات مرجعية تقود إلى الموضوعات ذات الصلة. ومن أهم المزايا التي تقدم,ها هذه الخدمة ميزة إنشاء

مواقع على الويب (Web Lunch) وادراجها في الدليل كما يتضمن دليلا بمواقع ويب الأكثر شعبية وقوائم بمواقع مميزة ومثيرة للإهتمام وينصح يزيارتها. وعنوان هذه الخدمة هو :

http://www. Yahoo.com

15- جوجل (google)

موقع جوجل هو أكثر موقع يفضله رواد الإنترنت حاليا ،ذلك لبساطة أسلوبه في البحث ولما يتوفر به من إمكانيات واسعة وأساليب بحث مريحة وهو من أكثر المواقع.عنوان الموقع

http://www. Google.com

3 - فهارس الإنترنت(Net):

يوجد صفحات من الويب تسمى فهارس(Directories) وهي من أهم الصفحات التي تساعد في عملية البحث عن موضوع عام   (General Topics) مثل الفنون و التعليم و الادارة و الانشطة و يحتوي الدليل على مواقع (Sites) مرتبة حسب الموضوع.

فمثلا يعرض دليل إكسيت (Excite) لمواقع تحوي موضوعات عديدة من بينها : الفنون – الأعمال – الحساب – التعليم – التسلية – الصحة والدواء – الأنشطة – المياه – المال و الاستثمار – الأخبار – الصفحات الشخصية – السياسة و القانون – الديانات -العلوم – التسوق – الرياضة.

و كما هو واضح تغطى هذه المواقع العديد من مجالات الاهتمام و تنتج عند الولوج إليها مصادر واسعة من المعلومات، و عند النقر عليها ستظهر لك قائمة بالموضوعات الفرعية المندرجة تحت الموضوع الأساسي، وهكذا تتفرع داخل القوائم حتى تصل إلى ما تبحث عنه، و فيما يلي نقدم بعض ادلة الانترنت الأكثر شعبية :

A2Z – Amazing Enviromental Organization Web Directory ! – Excite – Gamelan – Infoseek Guide – Magellan – Point – W3 Server – World Wide – Arts Resourees – Yahoo !

<u>نصائح مفيدة أثناء عملية البحث:</u>

آلة البحث او خدمة البحث تستخدم قاعدة بيانات عبارة عن فهرس يضم مجموعة من الكلمات او العبارات يصاحبها عناوين لمواقع على شبكة انترنت. و عند استخدامك لهذه الادوات يجب ان تراعي جيدا اختيار و وضع الكلمات المناسبة لكي يتم مطابقتها و الحصول على فائدة اكبر من عملية البحث، لذلك إليك سبعة نصائح مفيدة لتوفير اقصى استفادة من ادوات البحث :

اختار كلمات بحث مميزة و ليست دارجة، و كلما كانت الكلمة التي تدخلها مميزة و غير معتادة و تعبر عن حاجتك كلما كانت النتائج افضل و ادق و اسرع.

لا تستخدم لغة التخاطب العادية : بالرغم من ان بعض ادوات البحث تتيح لك استخدام اللغة العادية و التي تمكنك من ان تسأل عما تبحث و كأنك تحادث إنسان مثلك لكن يفضل دائما استخدام الكلمات الهامة التي تعبر عن موضوع بحثك.

استخدام اكثر من آلة بحث : كرر تجربة البحث باستخدام اكثر من آلة للتأكد من حصولك على افضل و اقرب النتائج.

اقرأ تعليمات استخدام آلة البحث : توفر في كل آلة مجموعة من التعليمات التي تساعدك في اجراء البحث بكفاءة مثل المعاملات (Operators) و المحددات (Delimiters) و قواعد البحث (Rules)، لذلك يجب ان تقرأ جيدا هذه التعلمات قبل استخدامك لآلة البحث.

الكلمات ذات المقطين : عند البحث عن كلمة ذات مقطعين مثل Turbo-Propeller حاول تجربة كل الاشكال الممكنة لكتابتها مثل :

Turbo-Propeller - Turbo-Propeller -Turbo-Propeller

استخدام المعاملات المنطقية : تدعم بعض آليات البحث استخدام المعاملات المنطقية، و ينصح باستخدام المعامل (Not) اذا كان متاحا و الذي يمكنك من اسبعاد احد من البحث : فمثلا عند البحث بالصيغة الآتية :

Aireaft NOT Civil Subsonic

فأنك تحصل على معلومات عن كل الطائرات و قد تم استبعاد المعلومات الخاصة بالطائرات المدنية.

7- احرص على ذكر البدائل و المرادفات : و قد يكون ما تبحث عنه موجود بإسم مرادف او اسم بديل لذلك إحرص على إدخال معظم الكامات التي تدل على ما تبحث عنه لكي يزيد فرصتك في الحصول عليه.

الإنترنت والبحث العلمي

اهتمت الإنترنت بمهارات البحث العلمي ودخول المكتبات العالمية، فأصبح من اليسير على الباحث الدخول إلى دليل المكتبة الإلكترونية، والبحث على رفوفها التي تحولت إلى خزائن، والتجول بها للحصول على المراجع العلمية المتخصصة التي تساعد الباحث في إعداد البحوث العلمية.

وقد ساهمت الإنترنت في ربط المكتبات في المؤسسات التعليمية بالمكتبات الخاصة بالباحثين والطلاب، حيث يسرت تداول المراجع العلمية الإلكترونية المتوفرة بالمكتبة، بحيث يستطيع الباحث الدخول إلى عناوين المراجع العلمية وتصفحها، والإلمام بالكتب التي تتناول نفس الموضوع الذي يبحث فيه وترتبط به إلكترونيا، وبهذه الطريقة السهلة يمكن إيجاد المصادر التعليمية المختلفة للبحث وتداولها عن طريق الإنترنت دون أن يفارق الباحث جهاز الكمبيوتر الشخصي بمكتبه.

الإنترنت والبحث العلمي.

(1) المكتبة الإلكترونية:

المكتبة الإلكترونية هي المكتبة التي ترتكز في عملها على تكنولوجيا المعلومات والاتصالات لتحويل بيانات المكتبة المختلفة وأسلوب العمل بها وتداول الكتب والدوريات والمجلات إلى أسلوب تقني يعتمد على التقنيات الحديثة وفي مقدمتها شبكة الإنترنت وخدماتها بغرض وتطوير البحث العلمي، وتيسير التجول بين المراجع العلمية المختلفة، والدخول إلى أجهزة الكمبيوتر بالمكتبات الأخرى لنقل المعلومات والمراجع أي إن كانت أماكن تواجدها.

أسباب ظهور المكتبات الإلكترونية:

هناك العديد من الأسباب التي أدت إلى ظهور المكتبة الإلكترونية ومن بينها.

تطور تكنولوجيا المعلومات والاتصالات وأهمية الاستفادة منها في مجالات المكتبات.

تطور مفهوم الفهرسة بظهور فهرسة شبكة الويب للوصول إلى مواقع المعلومات.

انتشار الأتمتة المكتبية office Automatic وذلك بإدخال أجهزة الحاسوب والشبكات المحلية في المكتبات التقليدية.

الرغبة في نشر محتويات المكتبات على متصفحي الإنترنت لجذب الباحثين إلى الجديد من الكتب والدوريات والمجلات العلمية.

الحاجة لدخول العاملين بالمكتبات إلى المكتبات الأخرى للحصول على المعلومات لمساعدة المترددين على المكتبات المحلية.

حاجة الباحثين والطلاب للدخول إلى المكتبات من أماكن تواجدهم في العمل أو المنزل للحصول على المعلومات المختلفة من المكتبات الإلكترونية المنتشرة في جميع أنحاء العالم.

فوائد المكتبة الإلكترونية:

تتضمن فوائد المكتبة الإلكترونية ما يلي:

يسرت مهارات تصنيف وفهرسة المراجع العلمية.

نشر المعلومات والمراجع العلمية على العالم ليستفيد منها الباحثين والطلاب والعامة.

يسرت للباحثين التجول بين عشرات المكتبات للبحث عن المراجع والدخول إلى خزائن المكتبات دون أن يترك مقعده أمام الكمبيوتر.

وفرت الدقة في المعلومات التي يحصل عليها الباحث.

خفضت تكاليف الحصول على المعلومات والمراجع العلمية.

اقتصدت في الوقت المستهلك للحصول على المعلومات والمراجع العلمية.

طرق الاتصال بالمكتبات الإلكترونية:

للحصول على المعلومات والمراجع والملفات من المكتبات الإلكترونية يجب استخدام أي من طرق الاتصال التالية:

البحث في مواقع الإنترنت. وذلك باستخدام فهرسة شبكات web وListserver وGopher للوصول إلى مواقع المعلومات والمراجع العلمية في المكتبات.

البريد الإلكتروني E- mail لإرسال الرسائل والملفات إلى المكتبة الإلكترونية بغرض الحصول على المعلومات والمراجع المتوفرة بها.

البريد الصوتي. وذلك لإرسال رسائل صوتية عن طريق الهاتف إلى المكتبة الإلكترونية حيث يتم تخزينها بالكمبيوتر أو الشبكة المحلية التي تربط بها المكتبة.

اجتماعات الفيديو Video Conferences حيث يتم الاتصال في اتجاه واحد أو اتجاهين عن طريق الإنترنت بالصوت والصورة لمناقشة المعلومات والمراجع العلمية المتوفرة بالمكتبة والحصول على أنسبها للبحث العلمي.

الكتاب الإلكتروني:

هو أسلوب جديد لعرض المعلومات بما تتضمنها من نصوص ورسومات وأشكال وصور وحركة ومؤثرات صوتية ولقطات فيلمية على هيئة كتاب متكامل يتم نسخه على الأقراص المدمجة CD-ROM.

المقارنة بين الكتاب الإلكتروني والكتاب التقليدي:

في هذه المقارنة يجب أن نوضح أن الكتاب الإلكتروني لم يتم كتابته على الورق بل سيتم نسخه على قرص، وهو لن يوضع على أرفف المكتبات بل سيتم وضعه بخزائن بالمكتبات، ولن يتم تصفحه باستخدام الأيدي بل سيتم تصفحه باستخدام الكمبيوتر، ولن يقتصر على النصوص والرسومات والصور بل سيحتوي إلى جانب ذلك على الصور المتحركة والمؤثرات الصوتية ولقطات من الأفلام، ولن يثقل كاهل الطالب بحمله إلى الجامعة أو المدرسة بل سيتم حفظه بحافظه صغيرة تحمل باليد.

خصائص الكتاب الإلكتروني:

الكتاب الإلكتروني هو الركيزة الأساسية التي تقوم عليها المكتبة الإلكترونية والكتاب الإلكتروني يتمثل في قرص مدمج CD-ROM تصل سعته القياسية إلى 650مجابايت، أي ما يقارب 675 مليون حرف، ولك أن تتخيل هذا العدد من الحروف إذا كان السطر يحتوي على 80 حرف، والصفحة الواحدة تحتوي على 32 سطر وبذلك يحتوي على ما يزيد على 360 ألف

صفحة من صفحات الكتاب التقليدي، وهو بذلك قد يحتوي القرص الواحد على ما يقارب 1000 كتاب حجم كل واحد منهم 360 صفحة.

هذا علما بأن تخزين الصور والأصوات والحركة ولقطات الأفلام وخلفيات الصفحات تحتاج إلى مساحات تخزين كبيرة مما يقلل من هذا العدد الضخم من الكتب الذي سبق ذكره والتي يمكن أن تحويها القرص المدمج الواحد، والآن ظهرت منذ عامين ونصف أقراص الفيديو الرقمية DVD التي تتمتع بسعة تخزين تزيد أكثر من عشرة أضعاف عن سعة القرص المدمج CD-ROM ويتم إعداد الكتاب الإلكتروني باستخدام لغة برمجة النص الفائق التداخل html حيث تتوفر من خلالها خاصية وصلات الترابط Links بين الأجزاء المختلفة لصفحات الكتاب، ومن ثم يتم الانتقال إلى أجزاء متفرقة من الكتاب بمجرد النقر بالفأرة على إحدى وصلات الترابط.

(3) الإنترنت والبحث العلمي:

لقد تغير مفهوم البحث العلمي في وجود الإنترنت، التي تطورت اهتماماتها بالمجالات المختلفة للبحث العلمي، فهي لم تقتصر على الاهتمام بأبحاث العلوم الأساسية، بل اهتمت بصورة مكثفة بأبحاث العلوم التربوية والإنسانية والاجتماعية، حيث عرضت نتائج البحوث المختلفة، وأصبح باستطاعة أي باحث نشر أبحاثه العلمية على العالم أجمع دون أية قيود، وبذلك تراكمت

المعلومات على الإنترنت بجميع أشكالها، وذلك ما لا يمكن لأي مكتبة تقليدية توفيره للباحثين وطلاب العلم.

أخلاقيات وقوانين الانترنت

ينبغي الالتزام بمجموعة من الأخلاق والآداب العامة. ومن هذا المنطلق، جاء مفهوم آداب الانترنت(Netiquette) المشتق من التعبير الإنجليزي **Net Etiquette** (أي السلوكيات المهذبة عند استخدام الانترنت)، ومن أهمها :

احترام الطرف الآخر: ينبغي عليك دائما أن تتذكر أن هنالك شخصا أو أشخاصا كثيرين على الطرف الآخر من الشبكة يتلقون رسائلك وأفكارك وآرائك، وأنه ينبغي عليك احترامهم و احترام أفكارهم وآرائهم.

الالتزام بعدم الإضرار بالآخرين:، ليس كما يفعل المخربون الإلكترونيين ويتم ذلك من خلال تجنب الآتي:

اختراق أجهزة الآخرين وسرقة مقتنياتهم وملفاتهم.

تدمير المواقع.

الاطلاع على كلمات السر التابعة للآخرين والمحافظة على سرية المعلومات.

إرسال برمجيات جافا (java Applets)،أو تحكمات (ActiveX)، والتي تؤدي إلى تخريب نظام التشغيل في جهازك، أو انتهاك خصوصياتك، باصطياد بعض المعلومات عنك.

عرض ملفات ملغومة بالفيروسات، بإمكانها إتلاف كل ما يتضمنه القرص الصلب، من بيانات وبرامج.

استغلال شبكة الانترنت في عمليات الاحتلال والتي تشمل : التزييف، الاعتداء، الاحتيال، و السرقة.

الايجاز في طرح الأفكار ومحاورة الآخرين فخير الكلام ما قل ودل.

تذكر دائما أنك عندما تقوم باستخدام الانترنت، فانك تصبح عضوا في مجتمع الانترنت، أي إنك تصبح Netizen (مشتقة من Net Citizen ومعناها مواطن انترنت أو عضو في مجتمع الانترنت)، وأن كل تصرف تقوم به يعبر عن شخصيتك، فاحرص دائما على تقديم الأفضل.

عدم السماح بنشر المعلومات الخاطئة كالافتراء/المعلومات الغير دقيقة/ العدائية/ التهديدية/ العنيفة.

عدم زيارة المواقع المحرمة والتي تخل بالشرف والنزاهة ومنها : مواقع الأفلام والصور الإباحية ومواقع تعليم الانتحار والسرقة والتجسس.

الالتزام بالقانون، فالتصرفات المخالفة للقانون في واقع الحياة تكون غالبا مخالفة للقانون على الانترنت.

احترام الحوارات القائمة بين الأشخاص والمجموعات، وتجنب مقاطعتها أو تعكير صفوها.

احترام الخصوصية الشخصية للآخرين، والإحجام عن اختراقها.

أخلاق البريد الالكتروني :

عند التخاطب- عبر الانترنت- بين فرد وجماعة أو بين جماعة وجماعة، تتزايد ضرورة الالتزام بمجموعة واسعة من الآداب والأخلاق؛ إذ إن أبسط الأخطاء قد يثير ردود أفعال واستنكارات أوسع بكثير مما قد يثيره في حالة حوار الفرد للفرد. وها نحن نذكر أنفسنا ونذكركم بأهمية هذه الآداب والأخلاق، ونورد منها ما يلي:

تجنب إثقال الوثائق الالكترونية بمعلومات التعريف الشخصية (Info Business Card)، وإن لم يكن هناك بد من إرسال العنوان فليكن على شكل ملف توقيع الكتروني (Electronic Signature file).

يجب توخي الحذر عند تحديد وجهة الوثيقة الالكترونية، لأن عناوين المجموعات تتشابه في شكلها مع عناوين الأفراد. تذكر أن لكل منهما خصوصيته التي يجب أن تصان.

التحقق من وجهة الرسائل التي تحتاج إجابة فورية ؛ لتحاشي إرسالها إلى منطقة زمنية بعيدة، فقد يحول هذا دون حصولك على الرد في وقته المناسب.

تضمين المراسلات الطويلة علامة في عنوانها، لكي يختار مستقبلها الوقت المناسب للاطلاع عليها. وفي المراسلات الإلكترونية، يصطلح أن تسمى الرسالة طويلة عندما تتجاوز مائة كلمة.

تحري الأساليب والكلمات المحافظة والمتفق عليها- إن كان لها مرجع - لأن مواطني الانترنت ينتمون إلى حضارات وبيئات متنوعة يجدر بمن أراد أن يكون منهم أن يراعيها.

عندما تكون الرسالة بلغة لا تينية الأصل، يجدر الابتعاد عن الصيغ غير المرغوب فيها عند بناء الوثائق الإلكترونية، مثل كتابة الوثيقة كاملة بحروف كبيرة ؛ لأن هذه الصيغة تشبه التوبيخ والعتاب الحاد.

تحاشي الخطابات الانفعالية، لما قد ينتج عنها من إساءات وندم.

تجنب استعمال النصوص المشفرة في كتابة الوثائق الإلكترونية،لأن ذلك يضيق على متلقيها الخناق في حال عدم حصوله على مفاتيح فك الشفرة، ويضيع الفائدة المرجوة منها.

الالتزام بتنسيق قياسي أثناء بناء الوثائق البريدية الالكترونية، ويشمل ذلك عدد الحروف في السطر الواحد (64 حرفا تقريبا في وثائق البريد الالكتروني)

وحجم الخط ونوعه، لأن عدم الالتزام بهذه القواعد قد يشوه الرسالة أو يفقدها جزءا مهما من محتواها، خاصة عندما يكون المستقبل من مستخدمي البرمجيات القديمة.

الابتعاد عن التزوير والخداع ؛ لأنهما أمران بغيضان يتعارضان مع الدين والأعراف والأخلاق الحميدة، ولأن يد القانون تطال المخالفين في العالم الالكتروني كما تطالهم في العالم التقليدي.

قبل الانخراط في النوادي والملتقيات الموجودة على الانترنت، ينبغي عليك أولا التحقق من توجهاتها وأفكارها ودرجة محافظتها على خصوصية أعضائها وآلية انتقائها لمصادر المعلومات التي يتم ربطها مع الأعضاء.

المحافظة على محتوى الرسالة الأصلية عند الرد عليها بطريقة الاعادة (Reply) أو التحويل) (Forward، لتساعد القارىء على تذكر أو معرفة موضوع الرسالة الأصلية وسبب الرد المرفق معها.

تفحص البريد الصادر دوريا للتأكد من وجهة الرسائل، وتوجيه كتب اعتذار إلى المجموعات والأفراد اللذين أرسلت إليهم بعض الوثائق الالكترونية بالخطأ.

التعامل بأمانة مع الوثائق الالكترونية التي تصل خطأ إلى صندوق البريد الالكتروني، وإعادتها إلى مرسليها، وعدم استغلال محتوياتها.

مناقشة شؤون المجموعة البريدية مع المسؤولين عن إدارة الشبكة المحلية، ويشمل ذلك قبول أو حجب التعامل مع بعض المجموعات الأخرى أو الأفراد أو إدراجهم في اللائحة السوداء التي تمنع وصول وثائقهم إلى العاملين في الشركة.

تحاشي استخدام أنواع غريبة من الخطوط والمخططات والرسوم المعقدة في الوثائق الالكترونية ؛ لأن ظهورها على أجهزة المتلقين سيكلفهم جهدا ووقتا، وقد لا يتمكن أغلبهم من فهم معانيها.

احترام حقوق الملكية الفكرية (Intellectual Property) في المواد المرسلة عبر البريد الالكتروني ؛ لأن الاستيلاء على النتاج العقلي والإنساني سرقة.

تجنب الرسائل المسلسلة(Chain letters)، وهي رسالة يبعث بها إلى مجموعة من الأشخاص على التوالي، ويقوم كل فرد من المجموعة بإرسالها إلى مجموعة أخرى, وفي معظم الأحيان، يغلب على هذه النوعية من المراسلات طيش الغاية وتفاهة المحتوى فهي تندرج في قائمة المحرمات على الانترنت ؛ لما تسببه من هدر للوقت ولموارد الشبكة.

تجنب إرسال قنابل البريد الالكتروني (email bombs) التي تتمثل في وصول مئات أو آلاف الرسائل إلى البريد الالكتروني، محدثة إزعاجا كبيرا للمستخدم.

الحرص على إضافة التوقيع الشخصي في خاتمة الوثائق الالكترونية لتعريف قارىء الوثيقة بك ؛ لأن الكثير من الشركات تمنح موظفيها عناوين الكترونية غامضة (أي تظهر للمستقبل على شكل أرقام ورموز لا تشير إلى شخص المرسل من قريب ولا بعيد).

تحري الأمانة في الوثائق الشعاعية (Threads) بنوعيها الخطية (من شخص واحد إلى شخص واحد) والتشعبية (من شخص واحد إلى عدة أشخاص)؛ وذلك بالمحافظة على الوثيقة الالكترونية الأصلية والردود المحتوية فيها دون أي تغيير، ليتمكن القارىء من متابعة الردود التي أرفقت بها.

احترام الخصوصية الشخصية (Privacy) لوثائق الآخرين التي قد تصلنا بالخطأ. وينبغي توجيه هذه الرسائل إلى العناوين الصحيحة أو إعادتها إلى عنوان المرسل.

الفصل الثاني

أمن المعلومات

مفهوم أمن المعلومات

هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها. ومن زاوية تقنية، هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية. ومن زاوية قانونية، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت).

واستخدام اصطلاح أمن المعلومات **Information Security** وان كان استخداما قديما سابقا لولادة وسائل تكنولوجيا المعلومات، الا انه وجد استخدامه الشائع بل والفعلي، في نطاق انشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال، اذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات- وتحديدا الإنترنت - احتلت ابحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات.

عناصر أمن المعلومات

ان اغراض ابحاث واستراتيجيات ووسائل أمن المعلومات – سواء من الناحية التقنية او الادائية - وكذا هدف التدابير التشريعية في هذا الحقل، ضمان توفر العناصر التالية لاية معلومات يراد توفير الحماية الكافية لها :-

السرية أو الموثوقية CONFIDENTIALITY : وتعني التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل اشخاص غير مخولين بذلك.

التكاملية وسلامة المحتوى INTEGRITY : التأكد من ان محتوى المعلومات صحيح ولم يتم تعديله او العبث به وبشكل خاص لن يتم تدمير المحتوى او تغيره او العبث به في اية مرحلة من مراحل المعالجة او التبادل سواء في مرحلة التعامل الداخلي مع المعلومات او عن طريق تدخل غير مشروع.

استمرارية توفر المعلومات او الخدمة AVAILABILITY :- التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض الى منع استخدامه لها او دخوله اليها.

عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation :- ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل

بالمعلومات او مواقعها انكار انه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة اثبات ان تصرفا ما قد تم من شخص ما في وقت معين.

المتطلبات الفنية لأمن المعلومات:

تعتبر مرحلة تحليل وتصميم امن النظام من أهم المراحل في بناء الأنظمة الآلية للمعلومات, بل وتقاس كفاءته الأمنية, وذلك لتداخل مرحلة تصميم امن النظام مع كل المراحل الأخرى وتأثيره فيها على ضوء تجارب المصممين للنظم الآلية للمعلومات عموما والمهتمين بمجال الأمن في النظم الآلية للمعلومات.

هناك عدة متطلبات فنية أساسية وضرورية لتصميم امن النظم الآلية للمعلومات وربما أهمها:

أ: الدراسة التحليلية لامن النظم:

إن الدراسة التحليلية لتحديد مناطق التهديد لأمن ومستوى الخطورة في كل منطقة ثم تصميم طرق الإنقاذ من كل منطقة من مناطق التهديد لابد إن تمثل جزءا أساسيا للغاية عند تحليل وتصميم النظام الآلي للمعلومات كما إن مستخدم النظام نفسه لابد إن يوثق الخطوات العملية التي يجب إن يقوم بها في أي حالة من حالات الكوارث في كتيب استخدام النظام.

ب: التوثيق:

أكدت كثير من الدراسات إن التوثيق في الأنظمة الآلية للمعلومات من اضعف الثغرات في امن تلك الأنظمة ويهدف التوثيق إلى جعل الأنظمة مفهومة للمستخدمين والمشغلين ومفهومة للمصممين حتى يمكنهم من الصيانة المستقبلية ومفهومة للمبرمجين حتى يتمكنون من صيانة البرامج على ضوء التصميم وغيرها من الصيانة العادية. إن جعل الأنظمة مفهومة للجميع كل في مجاله يحمي الأنظمة من احتكار أو ابتزاز المصمم الأساسي أو المبرمج الأساسي للأنظمة كما يجعل الاستخدام والتشغيل غير محتكرا لفئة محددة, لهذا يؤمن التوثيق الاستخدام الامثل والمستمر للأنظمة وهي غير معتمدة على أفراد. ومن ناحية أخرى يجب مراعاة إن التوثيق سلاح ذو حدين فيمكن إن يكشف التوثيق الممتاز الأنظمة لأشخاص غير مأذون لهم بذلك مما يستوجب عمل حماية خاصة وجيدة لوثائق النظام كما إن التوثيق الضعيف يمكن إن يؤدي إلى فقدان القدرة في التحكم مع استمرارية الزمن.

ج: امن البرامج والبيانات:

لقد لوحظ إن كثير من المبرمجين يقومون بعمل الصيانة العادية في البرامج على النسخ الأصلية للنظام فإذا حدثت أي مشكلة في برنامج ما يصعب عليهم بل قد يستحيل عليهم متابعة تلك المشكلة لعدم موافقة تلك البرامج موافقة تامة للوثيقة الأساسية للنظام. لهذا يجب المحافظة على النسخة الأصلية

للبرنامج المصدر وان يقوم المبرمجون بعمل اختباراتهم وبياناتهم على نسخة أخرى وعند الانتهاء من عمل الاختبارات وأجازة تشغيلها يتم تعديل النسخة الأصلية وتوثيق ذلك التعديل ثم نقلها إلى التنفيذ وبنفس الأسلوب يجب التعامل مع ملف البيانات خاصة الملفات الرئيسية فيجب تسجيل أي تغيير يحدث في محتويات تلك الملفات للمراجعة إذا لزم الأمر.

د: امن التشغيل:

يشمل امن التشغيل التحكم في الإدخال والتعديل والإطلاع في قسم المستخدمين والتنسيق بين قسم المستخدم والحاسب الآلي في توزيع المسؤوليات والتأكد من تشغيل الأعمال والبرامج الصحيحة في قسم الحاسب الآلي وضمان التشغيل المستمر للأجهزة متى طلب ذلك. نقطة الضعف في التشغيل هي عدم استيعاب المشغلين لظروف التشغيل استيعابا جيدا أو محاولة إثبات بعضهم عدم قدرة الأخر أو تغير أوقات الدوام أو ترك العمل. أما نقطة الضعف الأساسية في استمرارية عمل الحاسب الآلي تكمن في عدم التزام الشركات بعقود الصيانة.

ه: برامج امن النظام:

برامج امن النظام هي برامج مساعدة يتم تصميمها لتمكن من مراقبة أي تغيير في الملفات سواء كانت برامج أو بيانات ويتم ذلك بالطريقة الخاملة وهي تسجيل أي تغيير منذ البداية ليتم مراجعته مؤخرا أو بالطريقة الحية

وهي عدم السماح بالتغيير منذ البداية إلا بناء على صلاحية مبرمجة, إلا انه يجب الانتباه هنا إلى صعوبة التحكم في العاملين بالحاسب الآلي وخاصة المبرمجين نسبة لخبرتهم وقدرتهم على تجاوز هذه البرامج.

<u>و: الامن في نظم الاتصالات وقواعد البيانات:</u>

يشمل الأمن هنا التوثق من الطرفيات والمستخدمين وذلك بالتحكم الفيزيائي (سنتعرض له بشئ من التفصيل في مجال أخر) والتحكم المنطقي بعمل كلمات السر وربطها بنوع الاستخدام وتغييرها من وقت لأخر وبرمجة الطرفيات لتنفصل أليا إذا ظلت دون استخدام لفترة معينة أو إذا اخطأ المستخدم في كلمات عدة مرات.

كذلك يشمل الأمن في نظم الاتصال تسجيل كل الملاحظات في أي طرف ونوع الاستخدام إضافة بالطبع إلى التعرف على الشخص المستخدم عن طريق (رقم التعريف) والتوثق منه بكلمة السر أو البطاقة الممغنطة أو غيرها (التعرف) وربط ذلك بنوع من الاستخدام (الصلاحية) يتم ذلك في الغالب بتركيب أو تصميم نظام المعلومات بطريقة بنائية تكاملية يتم الانتقال فيه من بنية إلى أخرى عن طريق برامج تحكم خاصة تقوم بخزن معلومات عن الشخص الذي دخل إلى هذه البنية وتاريخ ووقت الدخول ونوع الحركة أو الاستخدام الذي قام به. هذه الخاصية متوفرة في كثير من نظم التشغيل

وبالأخص في نظم قواعد المعلومات حيث يشترك عدد ضخم من المستفيدين في التعامل مع قاعدة المعلومات كل في الجزئية والبنية التي تخصه.

ز: تطوير وتنفيذ النظم:

عند تطوير أو تصميم أي نظام يجب إتباع الطرق العلمية الصحيحة في التصميم كم يجب مراجعته جيدا واختباره والتأكد من خلوه من الأخطاء قبل بدء التنفيذ وكذلك يجب التأكد من تدريب موظفي التشغيل والاستخدام تدريبا جيدا يضمن تشغيلهم واستخدامهم للنظام بطريقة أمنة ومتدرجة قبل الاعتماد كليا عليه.

المتطلبات الإدارية لأمن المعلومات:

تكملة المتطلبات الفنية التي يجب مراعاتها في بناء النظم الآلية للمعلومات لحماية تلك النظم هناك عدة واجبات إدارية أهمها:

أ: التنظيم الاداري:

أولا: تنظيم إدارة خاصة بأمن النظم الآلية للمعلومات يناط بها تحديد الساسة الأمنية للنظام من حيث الإدخال, التعديل ومن حيث ضمان استمرارية العمل بالكفاءة المطلوبة. بعد تحديد هذه الساسة يجب توثيقها وتوقيعها بواسطة المسول الإداري للحاسب الآلي وكل العاملين والمستخدمين.

ثانيا: يحدد مشرفا للأمن بالحاسب الآلي تقع على عاتقه التأكد من التزام العاملين بالسياسة الأمنية المرسومة وتنسيق التدريب الفني في هذا المجال والمساعدة في التصميم والبرمجة لتنفيذ المتطلبات الفنية لهذه السياسة.

ثالثا: يحدد مسؤول امن يمثل المستخدم ويكون مسؤلا لدى الجهة المستخدمة للنظام من ضمان التزام إدارة الحاسب الآلي بالسياسة الأمنية المحددة وتحديد مستوى الصلاحية لكل المتعاملين مع النظام.

رابعا: يحدد قسم للمراجعة في إدارة الأمن مهمته عمل وتنفيذ نظام دقيق للمخزون من أجهزة وأشرطة وأقراص وتوثيق ومكتبات وقطع غيار وأوراق طباعة وحبر وغيرها من المستلزمات التشغيلية.

ب: خطط الطوارئ:

لابد من وضع الخطط لاستمرارية عمل النظام في حالة المشاكل الكبيرة كتعطل الحاسب الآلي تعطلا طويلا أو غير ذلك من الحالات الطارئة لابد من قياس المشاكل التي سيواجهها مستخدم النظام في هذه الحالات ووضع البدائل على ضوء ذلك فمثلا في النظم المصرفية أو نظم الحجوزات الجوية حيث لا غنى عن الحاسب الآلي ولو بضع دقائق يستوجب وجود نظام مساند يعمل بطريقة فورية في حالة الطوارئ في حين إن هناك أنظمة أخر يمكنها الاستغناء عن الحاسب الآلي عدة أيام دون إن تتأثر تأثرا كبيرا. هذا من ناحية الاستمرار التشغيلي المباشر للحاسب الآلي أما النواحي الأخرى

الهامة غير المباشرة أو المساندة كالكهرباء المستمرة والثابتة أو التبريد الموزون المستمر فهي ضرورية للتشغيل الخالي من الأخطاء إذ إن الزيادة الشديدة في التيار الكهربائي والارتفاع غير المحتمـل في درجات الحرارة كلها تؤدي إلى أخطاء في تشغيل ومعالجة البيانات. كذلك يجب مراعاة إن الانقطاع المفاجئ للتيار والإطفاء المباشر للحاسب الآلي كثيرا ما يؤدي إلى فقد بعض المعلومات أو السجلات.

ج: الامن الفيزيائي لمركز المعلومات والحاسب الالي:

يشمل الأمن الفيزيائي بمركز المعلومات والحاسب الآلي حمايته من الحريق والسوائل والغبار والكهرواستاتيكا وكذلك ضمان الكهرباء الكافية والمستلزمات البيئية من حرارة ورطوبة موزونة إضافة إلى التحكم في زيارة ودخول الأفراد إلى المبنى أو المكاتب أو إلى المكاتب الحساسة أو إلى مكتبات المراجع والأشرطة والأقراص ووثائق النظام أو إلى صالة الحاسب الآلي أو إلى طرفية المشغل أو إلى مفاتيح التبريد, كذلك التحكم في الوصول إلى المراكز الفرعية للطرفيات أو خطوط الاتصال أو غيرها من الأشياء المؤثرة في امن النظام الآلي للمعلومات.

د: مراقبة الأفراد:

يمثل الأفراد خط الدفاع الرئيسي في امن المعلومات خاصة المتعاملين مع النظام كما اشرنا سابقا.

فامن الأنظمة الآلية للمعلومات يعتمد أولا وأخيرا على أمانة الأفراد المتعاملين معها فلا يكفي التأكد من أخلاقيات الموظف وأهليته عند تعيينه بل يجب إن تستمر مراقبته لان التغيير السلوكي متوقع في أي وقت كذلك يجب عدم الاعتماد على موظف واحد بأي حال من الأحوال وان كان لابد من ذلك فيجب إن يشمل ذلك الموظف إشرافا ومراقبة دقيقة وتوثيقا دقيقا لأعمال وتدريب مساعدين لهم. عند انتهاء خدمات أي موظف يجب سحب صلاحيته قبل فترة كافية فهناك عدة حوادث انتقام من موظفين أنهيت خدماتهم.

ه: الصيانة والتامين:

تعتبر الصيانة خط الدفاع الثاني في امن الأنظمة الآلية للمعلومات ووجود الصيانة ضمان للتشغيل المستمر للأنظمة كما إن التامين التجاري يغطي تكلفة إرجاع المعلومات المفقودة وتغطية الخسارة الناتجة عن تعطيل النظام إضافة لتغطية الأجهزة إذا لم تغطى بواسطة عقود الصيانة.

و:- مراقبة المعالجة:

نعني بمراقبة المعالجة التأكد من المعالجة الصحيحة (الابتداء الصحيح للتشغيل) سواء كان إدخال أو تعديل أو استفسار ثم التوثق من إن هذه المعالجة تمت بإذن الجهات ذات الصلاحية (صلاحية التشغيل) ثم التأكد من إدخال الحركة هو الإدخال الصحيح وذلك بتكرار الإدخال مثلا وعمل

شاشة مختلفة لكل نوع من الإدخال إضافة لذلك لابد إن يكون للنظام خاصية التعرف على الأخطاء والتعرف على عدم الدقة في المعالجة وعمل تقرير بذلك, وأخيرا يجب إن تخدم التقارير المطبوعة أهداف محددة لإدارات محددة كما يجب تجنب الطباعة الزائدة التي قد تؤدي إلى تسرب المعلومات وضياع الورق. كذلك يجب إن تعكس التقارير المطبوعة الأنشطة المختلفة للأنظمة وتمثل بهذه مراجعة غير مباشرة للبيانات والمعالجة وحركة النظام بصفة عامة.

وصايا الاتحاد الدولي للاتصالات في امن المعلومات والاتصالات:

1-سلامة التركيب والصيانة بطرق سليمة : ان عدم التركيب والصيانة ان كان مقصود او غير مقصود يمثل مهدد امني كبير ويمكن ان يتم التواطؤ او مع الجهة التي تقوم بالتركيب والصيان لعمل اختراق او ممكن بسبب خطأ او ضعف في التركيب والصيانة يمكن العدو او المنافس من عمل الاختراق الأمني الذي يريده (الاختراق الأمني هو منع جهات مأذون لها بالتعامل او اتاحة التعامل مع جهات غير مأذون لها)

اذن المطلوب ان تقوم بالصيانة او التركيب جهات:-

مؤهلة علمياً ومهنياً وذات خبرة موثوقة

كذلك المطلوب عمل العقود القوية في التركيب والصيانة ومتابعة وتنفيذ تلك العقود

2- استخدام الجدران النارية وكلمات السر: ان الحوائط النارية قابلة للاختراق لذلك يجب تغييرها من وقت لآخر وفي فترات قصيرة ومثل ذلك كلمات السر يجب تبديلها من وقت لآخر وعدم تعريفها لاي شخص اخر مهما بلغت ثقتك منه كما يجب استخدام كلمات غير متوفرة في كلمات السر مثل (good morning،hello،sir)

ويجب ان يستخدم في النظام الهوية الالكترونية او الهوية البيلوجية اضافة لكلمة السر وهذا مايعرف بالثنائية الامنية.

3- التشفير : يجب استخدام التشفير متى ماتم التعامل مع الانترنت فعلى سبيل المثال التعامل مع الشبكات الافتراضية الخاصة ال (vpws) وبرنامج حماية بروتوكول الانترنت الافترضية (IP see) ويجب تغيير الشفرة بتكرارية عالية إعتماداً علي سرية المعلومة (الشبكة الامنية في تناقل المعلومة هي التي تستخدم شفرة جديدة مع كل رسالة (one pad key)).

4- اعطاء دور اوسع لمديري الشبكات : يجب أن يعلم مدير الشبكة بأنه هو المسئوول الأول والاساس من أمن الشبكة ومن ثم يتحمل هذه المسئولية ولابد ان تعطى له الصلاحية والامكانيات التي يطلبها ويضع

اللوائح والنظم والاجراءات الادارية التي تمكنه من ذلك إضافة الي المتطلبات التقنية.

5- إستخدام إستشاريين ومراجعيين من الخارج: إن مراجعة إجراءات الحماية والامنية بواسطة جهات خارجية متخصصة ضروري (لانه جل من لايسهو) ليكون ذلك رأياً آّخر او أن يؤكد على سلامة الاجراءات. كذلك المستشار أو المراجع يجب أن يكون مؤهلاً وموثوقاً (مراجعة خارجية).

6- المراجعة الدورية لاجراءات السلامة الأْمنية : يجب أن تكون هنالك مراجعة دورية كل شهر أو شهرين أو ثلاثة عن مدي سلامة الاجراءات الامنية وتحليل الاختراقات والمهددات الامنية. هذا بالطبع يتم بواسطة مسئولي الامن والحماية برئاسة مدير الشبكة داخل المؤسسة(مراجعة داخلية)

7- تحديد الاشخاص المخول لهم دخول غرفة المعلومات والشبكات: يجب إعطاء غرفة المعلومات والشبكات قدسيتها بإعتبارها المركز الرئيسي للاختراقات الامنية ولذا يجب تحديد اقل عدد ممكن من الاشخاص الذين يجوز لهم دخول الغرفة وكذلك المشرفين علي امنية النظام عموماً.

8- طلب معايير اعلى في برمجيات الامنية التجارية: ويجب أن يتم إقتناء برمجيات الأمنية من الشركات المؤهلة ذات الثقة العالية وذات الخبرة الطويلة في هذا المجال.

9- توعية وتثقيف المستخدمين (هندسة الامنية الاجتماعية) : يجب أن تتم توعية وتعريف المستخدمين بالمهددات الامنية وعدم تضليلهم (يعني يُتوهموا بأن شكل هذه الشفرة لايمكن كسرها وهذا النظام غير قابل للاختراق وان هنالك ضمان للأمن في شبكتنا كال ذلك كلام في غاية الخطورة لأنه من المعلوم في أمن المعلومات لاتوجد امنية مطلقة) إن توعية المستخدم بخطورة ومهددات امن المعلومات والاتصالات تجعله علي بينة من أمره اذا قرر التعامل مع النظام اوغير الشبكة فربما اذا علم ذلك ألا يتعامل مطلقاً مع الشبكة أو مع الانترنت في بعض اعماله.

10- تعميم الاجراءات الامنية المذكورة على كل المؤسسات مهما صغرت : إن الاجراءات الامنية التي تم ذكرها هي ليست للمؤسسات الكبري الحساسة فقط وإنما يجب أن تكون ثقافة وإلتزام عام في كل مؤسسة مهما صغرت ومهما قلت حساسيتها الامنية.

الفصل الثالث

الجريمة الإلكترونية

تتشابه الجريمة الالكترونية مع الجريمة التقليدية في إطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة و ضحية و الذي قد يكون شخص طبيعي أو شخص اعتباري و أداة و مكان الجريمة. وهنا يكمن الاختلاف الحقيقي بين نوعى الجريمة ففي الجريمة الالكترونية الأداة ذات تقنية عالية وأيضا مكان الجريمة الذي لا يتطلب انتقال الجاني إليه انتقالا فيزيقيا و لكن فى الكثير من تلك الجرائم فان الجريمة تتم عن بعد باستخدام خطوط و شبكات الاتصال بين الجاني و مكان الجريمة.

المفهوم القانوني للجريمة الإلكترونية :

تعرف الجريمة عموما، في نطاق القانون الجنائي : [4]- بأنها "فعل غير مشروع صادر عن ارادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا" [5].

وعلى الرغم من التبـاين الكبـير في تعريفـات الجريمـة بـين الفقهـاء القـانونين وبيـنهم وبـين علـماء الاجـتماع الا أننـا تخيرنـا هـذا التعريـف اسـتنادا الى أن

[4] الأستاذ الدكتور كامل السعيد ، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، الطبعة الثانية، دار الفكر للنشر والتوزيع ، عمان، 1983 .

[5] الأستاذ الدكتور محمود نجيب حسني، شرح قانون العقوبات - القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، 1989 ، ص 40 .

التعريف الكامل -كما يرى الفقه - هو ما حدد عناصر الجريمة الى جانب بيانه لأثرها[6].

أما جريمة الكمبيوتر، فقد صك الفقهاء والدارسون لها عددا ليس بالقليل من التعريفات، تتمايز وتتباين تبعا لموضع العلم المنتمية اليه وتبعا لمعيار التعريف ذاته، فاختلفت بين أولئك الباحثين في الظاهرة الاجرامية الناشئة عن استخدام الكمبيوتر من الوجهة التقنية وأولئك الباحثين في ذات الظاهرة من الوجهة القانونية.

يعرف **Sheldon. J. Hecht** الجريمة الإلكترونية بأنها: **"واقعة تتضمن تقنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب"**

وقد عرف جريمة الكمبيوتر خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية **OECD**، بانها **" كل فعل او امتناع من شانه الاعتداء على الأمواج المادية او المعنوية يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية "** [7]

[6] د محمود حسني ، السابق ، ص 40 ، و د.كامل السعيد ، السابق ، ص 28 .

[7] www.oecd.org

والتعريف البلجيكي السالف، متبنى من قبل العديد من الفقهاء والدارسين [8] بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الاحاطة الشاملة قدر الامكان بظاهرة جرائم التقنية، ولأن التعريف المذكور يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، ولأنه أخيرا يتيح امكانية التعامل مع التطورات المستقبلية التقنية.

ان الجرائم التي تطال ماديات الكمبيوتر ووسائل الاتصال، شأنها شأن الجرائم المستقرة على مدى قرنين من التشريع الجنائي، محلها أموال مادية صيغت على أساس صفتها نظريات وقواعد ونصوص القانون الجنائي على عكس (معنويات) الكمبيوتر ووسائل تقنية المعلومات، التي أفرزت أنشطة الاعتداء عليها تساؤلا عريضا - تكاد تنحسم الاجابة عليه بالنفي- حول مدى انطباق نصوص القانون الجنائي التقليدية عليه.

ويعرف خبراء منظمة التعاون الاقتصادي والتنمية، جريمة الكمبيوتر بأنها :

"كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/ أو نقلها" [9]

---

[8] د. رستم ، السابق ، ص 35 .

[9] انظر موقع المنظمة على شبكة الانترنت – مشار اليه فيما سبق .

وقد وضع هذا التعريف من قبل مجموعة الخبراء المشار اليهم للنقاش في اجتماع باريس الذي عقد عام 1983 ضمن حلقة (الاجرام المرتبط بتقنية المعلومات)، ويتبنى هذا التعريف الفقيه الالماني **Ulrich Sieher**، ويعتمد هذا التعريف على معيارين : أولهما، (وصف السلوك). وثانيهما، اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

ومن ضمن التعريفات التي تعتمد أكثر من معيار، يعرف جانب من الفقه جريمة الكمبيوتر وفق معايير قانونية صرفه، أولها تحديد محل الجريمة، وثانيها وسيلة ارتكابها وهو في كلا المعيارين (الكمبيوتر) لما يلعبه من دور الضحية ودور الوسيلة حسب الفعل المرتكب كما يرى هذا الجانب من الفقه.

و يعرف الفرنسي، Masse جريمة الكمبيوتر بأنها **"الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"** [10] وجرائم الكمبيوتر في هذا التعريف جرائم ضد الأموال.

ان طبيعة وأبعاد ظاهرة جرائم الكمبيوتر، سيما في ظل تطور انماطها يوما بعد يوم مع تطور استخدام الشبكات وما اتاحته الإنترنت من فرص جديدة لارتكابها وخلقت انماطا مستجدة لها يشير الى تميزها في احكام لا توفرها النظريات القائمة، تحديدا مسائل محل الاعتداء والسلوكيات المادية المتصلة بارتكاب الجرم، وهذا ما أدى الى حسم الجدل الواسع حول مدى انطباق

[10] انظر د. الشوا ، السابق ، ص 3 .

النصوص القائمة على هذه الجرائم لجهة وضع تشريعات ونصوص جديدة تكون قادرة على الاحاطة بمفردات ومتطلبات وخصوصية جرائم الكمبيوتر والإنترنت، وهو بالتالي ما يحسم الجدل حول الحاجة الى نظرية عامة لجرائم الكمبيوتر توقف التوصيف الجزئي والمعالجات المبتسرة.

اما عن دور الكمبيوتر في الجريمة ، فانه متعدد في الحقيقة، فهو اما ان يكون الهدف المباشر للاعتداء، او هو وسيلة الاعتداء لتحقيق نتيجة جرمية لا تتصل مباشرة بالمعطيات وانما بما تمثله او تجسده، او هو بيئة ومخزن للجريمة، ويجب أن لا يوقعنا أي من هذه الادوار في أي خلط بشان محل الجريمة أو وسيلة ارتكابها، فان محل جريمة دائما هو المعطيات (أما بذاتها أو بما تمثله) ووسيلة ارتكاب جريمة الكمبيوتر والإنترنت الكمبيوتر او أي من الاجهزة التكاملية التقنية (أي التي تدمج بين تقنيات الاتصال والحوسبة) وعلى أن يراعى ان دلالة نظام الكمبيوتر تشمل نظم تقنية المعلومات المجسدة في الكمبيوتر المحقق لتوأمة الحوسبة والاتصال في عصر التقنية الشاملة المتقاربة.

ان مفهوم جريمة الكمبيوتر مر **بتطور تاريخي** تبعا لتطور التقنية واستخداماتها، ففي المرحلة الأولى من شيوع استخدام الكمبيوتر في الستينات ومن ثم السبعينات، ظهرت اول معالجات لما يسمى جرائم الكمبيوتر - وكان ذلك في الستينات - واقتصرت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر، وترافقت هذه

النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة جرمية مستجدة، بل ثار الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير اخلاقية في بيئة او مهنة الحوسبة، وبقي التعامل معها اقرب الى النطاق الاخلاقي منه الى النطاق القانوني، ومع تزايد استخدام الحواسيب الشخصية في منتصف السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية ، وبدأ الحديث عنها بوصفها ظاهرة جرمية لا مجرد سلوكيات مرفوضة. وفي الثمانينات طفا على السطح مفهوم جديد لجرائم الكمبيوتر ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد وانشطة نشر وزراعة الفايروسات الإلكترونية، التي تقوم بعمليات تدميرية للملفات او البرامج، وشاع اصطلاح (الهاكرز) المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل في غالب الاحيان محصورا بالحديث عن رغبة المخترقين في تجاوز إجراءات أمن المعلومات وفي اظهار تفوقهم التقني، وانحصر الحديث عن مرتكبي الأفعال هذه بالحديث عن صغار السن من المتفوقين الراغبين بالتحدي والمغامرة والى مدى نشأت معه قواعد سلوكية لهيئات ومنظمات الهاكرز طالبوا معها بوقف تشويه حقيقتهم واصرارهم على انهم يؤدون خدمة في التوعية لأهمية معايير أمن النظم والمعلومات لكن الحقيقة ان مغامري الامس اصبحوا عتاة اجرام فيما بعد، الى حد إعادة النظر في تحديد سمات مرتكبي الجرائم وطوائفهم، وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض جرمية خطرة، القادر على ارتكاب أفعال

تستهدف الاستيلاء على المال او تستهدف التجسس او الاستيلاء على البيانات السرية الاقتصادية والاجتماعية والسياسية والعسكرية. وشهدت التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وكان ذلك بفعل ما احدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات، فظهرت انماط جديدة كانشطة انكار الخدمة التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد، واكثر ما مورست ضد مواقع الإنترنت التسويقية الناشطة والهامة التي يعني انقطاعها عن الخدمة لساعات خسائر مالية بالملايين. ونشطت جرائم نشر الفايروسات عبر مواقع الإنترنت لما تسهله من انتقالها الى ملايين المستخدمين في ذات الوقت، وظهرت انشطة الرسائل والمواد الكتابية المنشورة على الإنترنت او المرسلة عبر البريد الإلكتروني المنطوية على اثارة الاحقاد او المساس بكرامة واعتبار الأشخاص او المستهدفة الترويج لمواد او أفعال غير قانونية وغير مشروعة (جرائم المحتوى الضار).

ان تعريف الجريمة عموما يتأسس على بيان عناصرها المناط بالقانون تحديدها، اذ من دون نص القانون على النموذج القانوني للجريمة لا يتحقق امكان المساءلة عنها (سندا الى قاعدة الشرعية الجنائية التي توجب عدم جواز العقاب عند انتفاء النص، وسندا الى ان القياس محظور في ميدان النصوص التجريمية الموضوعية)، وهو ما يستوجب التمييز بين الظاهرة الجرمية والجريمة.

دور الكمبيوتر في الجريمة

يلعب الكمبيوتر ثلاثة ادوار في ميدان ارتكاب الجرائم، ودورا رئيسا في حقل اكتشافها، ففي حقل ارتكاب الجرائم يكون للكمبيوتر الادوار التالية :-

الاول:- قد يكون الكمبيوتر هدفا للجريمة (Target of an offense)، وذلك كما في حالة الدخول غير المصرح به الى النظام او زراعة الفايروسات لتدمير المعطيات والملفات المخزنة او تعديلها، وكما في حالة الاستيلاء على البيانات المخزنة او المنقولة عبر النظم.

ومن اوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية، عندما تكون السرية (CONFIDENTIALITY) والتكاملية أي السلامة (INTEGRITY) والقدرة أو التوفر AVAILABILITY) هي التي يتم الاعتداء عليها، بمعنى ان توجه هجمات الكمبيوتر الى معلومات الكمبيوتر او خدماته بقصد المساس بالسرية او المساس بالسلامة والمحتوى والتكاملية، او تعطيل القدرة والكفاءة للانظمة للقيام باعمالها، وهدف هذا النمط الاجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون تخويل ودون ان يدفع الشخص مقابل الاستخدام (سرقة خدمات الكمبيوتر، او وقت الكمبيوتر) او المساس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر وغالبية هذه الأفعال الجرمية تتضمن ابتداءا الدخول غير المصرح به الى النظام الهدف (UNAUTHORIZED ACCESS) والتي توصف بشكل

شائع في هذه الايام بأنشطة الهاكرز كناية عن فعل الاختراق (HACKING).

والافعال التي تتضمن سرقة للمعلومات تتخذ اشكال عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء، فالكمبيوترات مخازن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق وغيرها وهذه تمثل هدفا للعديد من الجهات بما فيها ايضا جهات التحقيق الجنائي والمنظمات الارهابية وجهات المخابرات والاجهزة الامنية وغيرها، ولا يتوقف نشاط الاختراق على الملفات والانظمة غير الحكومية بل يمتد الى الانظمة الخاصة التي تتضمن بيانات قيمة، فعلى سبيل المثال قد يتوصل احد المخترقين للدخول الى نظام الحجز في احد الفنادق لسرقة ارقام بطاقات الائتمان. وتتضمن بعض طوائف هذا النمط أي الكمبيوتر كهدف انشطة سرقة والاعتداء على الملكية الفكرية كسرقة الاسرار التجارية واعادة انتاج ونسخ المصنفات المحمية وتحديدا برامج الحاسوب. وفي حالات اخرى فان افعال الاختراق التي تستهدف انظمة المعلومات الخاصة تستهدف منافع تجارية او ارضاء اطماع شخصية كما ان الهدف في هذه الطائفة يتضمن انظمة سجلات طبية وانظمة الهاتف وسجلاته ونماذج تعبئة البيانات للمستهلكين وغيرها.

الثاني :- وقد يكون الكمبيوتر اداة الجريمة لارتكـــاب جرائم تقليدية A tool in the commission of a traditional offense

كما في حالة استغلال الكمبيوتر للاستيلاء على الأموال باجراء تحويلات غير مشروعة او استخدام التقنية في عمليات التزييف والتزوير، او استخدام التقنية في الاستيلاء على ارقام بطاقات ائتمان واعادة استخدامها والاستيلاء على الاموال بواسطة ذلك، حتى ان الكمبيوتر كوسيلة قد يستخدم في جرائم القتل، كما في الدخول الى قواعد البيانات الصحية والعلاجية وتحويرها او تحوير عمل الاجهزة الطبية والمخبرية عبر التلاعب ببرمجياتها، او كما في اتباع الوسائل الالكترونية للتأثير على عمل برمجيات التحكم في الطائرة او السفينة بشكل يؤدي الى تدميرها وقتل ركابها.

الثالث :- وقد يكون الكمبيوتر بيئة الجريمة، وذلك كما في تخزين البرامج المقرصنة فيه او في حالة استخدامه لنشر المواد غير القانونية او استخدامه اداة تخزين او اتصال لصفقات ترويج المخدرات وانشطة الشبكات الاباحية ونحوها.

وطبعا يمكن للكمبيوتر ان يلعب الادوار الثلاثة معا، ومثال ذلك ان يستخدم احد مخترقي الكمبيوتر (هاكرز) جهازه للتوصل دون تصريح الى نظام مزود خدمات انترنت (مثل نظام شركة امريكا اون لاين) ومن ثم يستخدم الدخول غير القانوني لتوزيع برنامج مخزن في نظامه (أي نظام المخترق) فهو قد ارتكب فعلا موجها نحو الكمبيوتر بوصفه هدفا (الدخول غير

المصرح به) ثم استخدم الكمبيوتر لنشاط جرمي تقليدي (عرض وتوزيع المصنفات المقرصنة) واستخدم كمبيوتره كبيئة او مخزن للجريمة عندما قام بتوزيع برنامج مخزن في نظامه.

اما من حيث دور الكمبيوتر في اكتشاف الجريمة، فان الكمبيوتر يستخدم الان على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم، عوضا عن ان جهات تنفيذ القانون تعتمد على النظم التقنية في ادارة المهام من خلال بناء قواعد البيانات ضمن جهاز ادارة العدالة والتطبيق القانوني، ومع تزايد نطاق جرائم الكمبيوتر، واعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة، فانه اصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها، من هنا يلعب الكمبيوتر ذاته دورا رئيسا في كشف جرائم الكمبيوتر وتتبع فاعليها بل وابطال اثر الهجمات التدميرية لمخترقي النظم وتحديدا هجمات الفيروسات وإنكار الخدمة وقرصنة البرمجيات.

الركن المادي في جرائم الإنترنت:

إن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية واتصال بالانترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته. فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة. فيقوم بتحميل الحاسب ببرامج اختراق، او أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلي تهيئة صفحات تحمل في طياتها مواد

داعرة أو مخلة بالآداب العامة وتحميلها علي الجهاز المضيفHosting Server ، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.

ليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والانترنت – حتى ولو كان القانون لا يعاقب علي الأعمال التحضيرية- إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشئ. فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للاطفال فمثل هذه الاشياء تمثل جريمة في حد ذاتها.

تثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة، فعلي سبيل المثال مكان وزمان تحقق النتيجة الإجرامية. فلو قام احد المجرمين في أمريكا اللاتينية باختراق جهاز خادم Serverاحد البنوك في الأمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين، ويثور أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن. حيث أن هناك بعد دولي في هذا المجال.

الركن المعنوي في جرائم الإنترنت:

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي

للجريمة بين مبدأ الإرادة ومبدأ العلم. فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحيانا أخري اخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي.

برزت تلك المشكلة في قضية موريس الذي كان متهما في قضية دخول غير مصرح به علي جهاز حاسب فيدرالي وقد دفع محامي موريس علي انتفاء الركن المعنوي، الأمر الذي جعل المحكمة تقول " هل يلزم أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به، بحيث تثبت نية المتهم في الولوج إلي حاسب فيدرالي، ثم يلزم إثبات نية المتهم في تحدي الحظر الوارد علي استخدام نظم المعلومات في الحاسب وتحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلي تحديد أركان جريمة الدخول دون تصريح ". وبذلك ذهبت المحكمة إلي تبني معيارين هنا هما الإرداة بالدخول غير المصرح به، وكذا معيار العلم بالحظر الوارد علي استخدام نظم معلومات فيدرالية دون تصريح.

أما بالنسبة للقضاء الفرنسي فإن منطق سوء النية هو الأعم في شان جرائم الانترنت، حيث يشترط المشرع الفرنسي وجود سوء نية في الاعتداء علي بريد إلكتروني خاص بأحد الأشخاص.

هذا ويمكن القول أيضا بتوافر الركن المعنوي في جرائم الانترنت في المثال التالي، قيام أحد القراصنة بنسخ برامج كمبيوتر من موقع علي شبكة

الانترنت، والقيام بفك شفرة الموقع وتخريبه للحصول علي البرمجيات ولإيقاع الأذى بالشركة .

المسئولية الجنائية في الجرائم المرتكبة عبر الانترنت:

إن الوصول للمجرم المعلوماتي أو الإلكتروني يشكل عبء فني وتقني بالغ علي القائمين بأعمال التتبع والتحليل لملابسات الوقائع الإجرامية المختلفة. وقد نصت المادة 12 من معاهدة بودابست لمكافحة جرائم الفضاء المعلوماتي على:

-سوف يتبنى كل طرف تدابير تشريعية، وأي تدابير أخرى لضمان قيام مسئولية الأشخاص المعنوية عن أي جريمة موصوفة في هذه المعاهدة إذا ما ارتكبت لصالح الشخص المعنوي بواسطة شخص طبيعي اقترفها بشكل منفرد أو بوصفه جزء من عضو في الشخص المعنوي على أساس من:

- •تفويض من الشخص المعنوي
- •سلطة اتخاذ قرارات لصالح الشخص المعنوي
- •سلطة لممارسة رقابة أو سيطرة داخل الشخص المعنوي

-إلى جانب الحالات الواردة في البند 1 سوف يتخذ كل طرف التدابير اللازمة لضمان قيام مسئولية الشخص المعنوي إذا ما أدى نقص الإشراف أو السيطرة من قبل الشخص الطبيعي المشار إليه في الفقرة 1 إلى إمكانية ارتكاب جريمة قائمة طبقا لهذه المعاهدة لصالح الشخص المعنوي بواسطة شخص

طبيعي اقترفها تحت سيطرته.

-هذه المسئولية لن تؤثر على قيام المسئولية الجنائية للأشخاص الطبيعيين الذين اقترفوا الجريمة

مسئولية مقدمي خدمة الوصول للإنترنت

تتعدد طرق الوصول إلي الانترنت سواء علي طريق Dial Up , Leased Line, IDSL, ISDN، إلا إنه في كل الأحوال يجب وجود مقدم خدمةInternet Service Provider ، ولقد أثارت مسألة مقدم الخدمة باعتباره فاعل اصلي في الجريمة الكثير من الجدل ويري اتجاه من الفقهاء عدم مسئوليته تأسيساً علي أن عمله فني وليس في مقدوره مراقبة المحتوي المقدم ولا متابعة تصرفات مستخدم الانترنت .

ويرى الاتجاه الثاني مسائلته تأسيساً علي أسس المسئولية التوجيهية فإنه يتعين علي مقدم الخدمة منع نشر محتوى صفحات الشبكة المتعارضة مع القوانين والنظم واللوائح او المصلحة العامة.

ويذهب القضاء الفرنسي أن مجرد قيام مستخدم الشبكة ببث رسالة غير مشروعة لا يكفي لقيام مسئولية مقدم خدمة الانترنت وذلك أخذا في الاعتبار العدد اللانهائي للمشتركين وحجم الرسائل الرهيب المتداول يوميا.

مسئولية مقدم الاستضافة

عن مقدم خدمة الاستضافة هو الشركة التي تستضيف مواقع الانترنت علي خوادمها Serversويكون مقدم الخدمة مؤجر وصاحب الموقع مستأجر لمساحة معينة على الجهاز الخادم الخاص بالشركة، والمستخلص من أحكام القضاء والفقه المقارن قيام مسئولية متعهد أو مقدم خدمة الاستضافة إذا كان يعلم، أو كان عليه أن يعلم بالجريمة ولم يتخذ الإجراءات اللازمة لوقفها .

سمات ودوافع الجريمة المعلوماتية :

تتسم الجريمة المعلوماتية بصفات تميزها عن الجرائم التقليدية هي التالية :

1. تقع الجريمة في بيئة المعالجة الآلية للبيانات ,حيث يستلزم لقيامها التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي بغرض معالجتها الكترونياً ,بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة والتي يتوافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها وطباعتها وهذه العمليات وثيقة الصلة بارتكاب الجريمة, ولابد من فهم الجاني لها أثناء ارتكابها في حالات التزوير والتقليد.

2. إثبات تلك الجرائم يحيط به كثير من الصعوبات التي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثراً خارجياً, فلايوجد جثث لقتلى أو أثاراً لدماء وإذا اكتُشفت جريمة فلايكون ذلك إلا بمحض الصدفة, والدليل

على ذلك أنه لم يُكتشف منها إلا نسبة 1% فقط, والذي تم الإبلاغ عنه للسلطات المختصة لا يتعدى 15 % من النسبة السابقة.

3. أدلة الإدانة فيها غير كافية إلا في حدود 20% فقط, ويرجع ذلك إلى عدة عوامل تتمثل في عدم وجود أي أثر كتابي ,إذ يتم نقل المعلومات بالنبضات الالكترونية,كما وأن الجاني يستطيع تدمير دليل الإدانة ضده في أقل من ثانية.

4. إحجام الشركات والمؤسسات في مجتمع الأعمال عن الإبلاغ عما يُرتكب داخلها من جرائم تجنباً للإساءة إلى السمعة وهز الثقة فيها.

5. هذه الجرائم لا تعرف الحدود بين الدول والقارات حيث أن القائم على النظام المعلوماتي في أي دولة يمكنه أن يحول مبلغاً من المال لأي مكان في العالم مضيفاً له صفر أو بعض الأصفار لحسابه الخاص , بل يستطيع أي شخص أن يعرف كلمة السر لأي شبكة في العالم ويتصل بها ويغير ما بها من معلومات.

6. الرغبة في استقرار حركة التعامل ومحاولة إخفاء أسلوب الجريمة حتى لا يتم تقليدها من جانب الآخرين , كل ذلك يدفع المجني عليه إلى الإحجام عن مساعدة السلطات المختصة في إثبات الجريمة أو الكشف عنها , حتى في حالة الضبط لا يتعاون مع جهات التحقيق خوفاً مما يترتب على ذلك من دعاية

مضادة وضياع الثقة ,حيث يكون المجني عليه في مثل هذه الحالة بنك أو مؤسسة مالية([11]).

مرتكبو الجريمة المعلوماتية :

إن مرتكبي جرائم الحاسوب عموماً، ينتمون وفق الدراسات المسحية إلى فئة عمرية تتراوح بين (25- 45) عاما, ويتميز هؤلاء بسمات عامة , يمكن النظر إليها من زاويتين:

1-: الصفات الشخصية والتخصص والكفاءة :

الجامع بين محترفي الجرائم المعلوماتية، تمتعهم بقدرة عالية من الذكاء، وإلمام جيد بالتقنية العالية، واكتسابهم معارف عملية وعلمية، وانتمائهم إلى التخصصات المتصلة بالحاسوب من الناحية الوظيفية، وهذه السمات تتشابه مع سمات مجرمي ذوي الياقات البيضاء.

كما أن مرتكبي هذا النوع من الجرائم المعالجة الآلية للمعلومات يتميزون في غالب الأحيان بأنهم أفراد ذوي مكانة في المجتمع ([12]), فغالباً ما يكون

[11] د أحمد خليفة الملط " الجرائم المعلوماتية" - دار الفكر الجامعي ,الإسكندرية ,الطبعة الثانية 2006م .ص 83 وما بعدها

[12] د جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي- دار النهضة العربية،،القاهرة ,الطبعة الأولى، 1992م ص 15.

هؤلاء من أصحاب الوظائف الحيوية والمفصلية في أماكن عملهم ,سواء في بيئة القطاع الخاص كالشركات والمؤسسات والمنشات الاقتصادية والمصارف الخاصة , أو في القطاع العام وأجهزته من وزارات وهيئات حكومية أخرى.

2- من حيث الجوانب السيكولوجية:

إن الدراسات القليلة للجوانب السيكولوجية للمجرمين المعلوماتيين، أظهرت شيوع عدم الشعور بلا مشروعية الطبيعة الإجرامية وبلا مشروعية الأفعال التي يقترفونها، كذلك الشعور بعدم استحقاقهم للعقاب عن هذه الأفعال، فحدود الشر والخير متداخلة لدى هذه الفئة، وتغيب في دواخلهم مشاعر الإحساس بالذنب، وهذه المشاعر في الحقيقة تبدو متعارضة.

وقد حدد Donn Parker وهو مختص في تحليل الجريمة المعلوماتية في معهد (stannifère) سبعة أصناف للمجرمين المعلوماتيين وهم :

· الهواة.

· المهووسون : وهم الذين يرتكبون الجريمة باستخدام العنف الذي يصعب تصوره في المجال المعلوماتي , فالحالة الكلاسيكية الوحيدة لهذه الطائفة من المجرمين المعلوماتيين هي حالة المبرمج المجنون الذي يهدف إلى تحطيم كل الأنظمة.

· الجريمة المنظمة: فجهاز الحاسوب أصبح أداة فعالة بأيدي بارونات الجريمة المنظمة وعصابات المافيا.

· الحكومات الأجنبية : والتي تستعمل أجهزة الحاسب في مجال الجاسوسية.

· النخبة.

· المتطرفون : والذين يستخدمون الشبكات المعلوماتية لنشر أفكارهم السياسية والدينية المتطرفة.

· مخربو الأنظمة المعلوماتية ([13]).

الدوافع لارتكاب الجريمة المعلوماتية :

تتلخص الدوافع الكامنة وراء هذا النمط المستحدث من الإجرام بالنقاط التالية:

1- الكسب المادي(الربح): إذ قد يحدث أن يستهدف مرتكبو هذا النوع من الجرائم تحقيق نفع مادي,خصوصاً أن النفع المادي الناتج عن هذه الجرائم يعد مغرياً , إذا قد يصل إلى أكثر من 50 ضعف الحصيلة الناتجة عن ارتكاب الجرائم التقليدية التي يكون غرضها تحقيق نفع مادي.

[13] قارة أمال – الجريمة المعلوماتية – رسالة ماجستير مقدمة لكلية الحقوق بجامعة الجزائر للعام الدراسي 2002 , ص 27 , موجودة كنسخة الكترونية على الموقع الإلكتروني التالي : WWW.4Shared.com

2- الثأر من المنشأة: ذلك أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية وعن طبيعة علاقات العمل المنفرة في حالات معينة، هذه الأمور قد تمثل في حالات كثيرة قوة محركة لبعض العاملين لارتكاب جرائم معلوماتية، باعثها الانتقام من المنشأة أو رب العمل.

3- التحدي الذهني : إذ قد تُرتكب هذه الجرائم بهدف قهر النظام المعلوماتي , الذي يرى الجاني في تعقيد أجهزته وأنظمته الأمنية , وما أحيط حوله من هالة عن قدراته , موضوعاً يستفز مهاراته وإمكاناته ويثير رغبة التحدي لديه.

4- دوافع أخرى: الدوافع المذكورة أعلاه تعد أبرز دوافع ارتكاب الجريمة المعلوماتية، لكنها ليست كل الدوافع، فمحرك أنشطة الإرهاب الالكتروني وحروب المعلومات على سبيل المثال هي الدوافع السياسية والإيديولوجية، في حين أن أنشطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة، والفعل الواحد قد يعكس دوافع متعددة خاصة إذا ما اشترك فيه أكثر من شخص انطلق كل منهم من دوافع خاصة به وتختلف عن غيره.

أنواع الجريمة الإلكترونية:

أولاً : جرائم الاعتداء على الحياة الخاصة للأفراد

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقلدية، فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك ومناقشة الحالات التي تثير مشكلة في تطبيق النصوص التقليدية وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم وهي جرائم الاعتداء على الحياة الخاصة.

يصعب بداية حصر عناصر الحق في الحياة الخاصة فهي تتكون من عناصر ليست محل اتفاق بين الفقهاء فيمكن القول بأنها تشمل حرمة جسم الإنسان والمسكن والصورة والمحادثات والمراسلات والحياة المهنية[14].

اما علاقة الحياة الخاصة بالتقنية المعلوماتية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الاونه الاخيرة لخدمة اغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية[15].

[14] ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائي – دار النهضة العربية القاهرة 1983 ص 207

هكذا اصبحت الشبكات المعلوماتية مستودعا خطيرا للكثير من اسرار الانسان التي يمكن الوصول اليها بسهولة وسرعة لم تكن متاحة في ظل سائر وسائل الحفظ التقليدية فأصبحت بنوك المعلومات أهم وأخطر عناصر الحياة الخاصة للإنسان في العصر الحديث.

وقد كان ذلك في البداية بالنسبة للمعلومات التي يدلي بها بعض الأشخاص بإرادتهم الخاصة أثناء تعاملاتهم مع المؤسسات العامة والخاصة في البنوك و المؤسسات المالية كمؤسسات الائتمان وشركات التأمين والضمان الاجتماعي وغيرها،فالبيانات الخاصة بشخصية المستخدم يمكن الوصول اليها عن طريق زيارة بعض المواقع على شبكة المعلومات، لان شبكات الاتصال تعمل من خلال بروتوكولات موحدة تساهم في نقل المعلومات بين الاجهزة وتسمى هذه البروتوكولات الخاصة مثل بروتوكولات HITP الذي يمكن عن طريقها الوصول الى رقم جهاز الحاسب الشخصي ومكانه وبريده الالكتروني، كما ان هناك بعض المواقع التي يؤدي الاشتراك في خدماتها الى وضع برنامج على القرص الصلب للحاسب الشخصي وهو ما يسمى cookies وهدفه جمع معلومات عن المستخدمين . بل ان اخطر ما في استخدام هذه الشبكة يتمثل في ان كل ما يكتبه الشخص من رسائل يحفظ في ارشيف خاص يسمح

[15] أسامة عبد اللـه قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية القاهرة 1994 ص 48

بالرجوع اليه ولو بعد عشرون عاما[16]. ويظن الكثيرون ان الدخول باسم مستعار او بعنوان بريدي زائف لساحات الحوار ومجموعات المناقشة قد يحميهم ويخفي هويتهم، وفي الحقيقة فإن مزود الخدمة او internet service provider (ISP) يمكنه الوصول إلى كل هذه المعلومات بل ويمكنه أيضا معرفه المواقع التي يزورها العميل.

ثانيا جرائم الاعتداء على الأموال:

إذا كان قانون العقوبات الليبي شأنه شأن كل قوانين العقوبات الأخرى قد جرم الاعتداء على الأموال في صوره التقليدية كالسرقة والنصب وخيانة الأمانة واختلاس الأموال العامة، فقد كان ذلك في ظل عصر لا يعرف سوى النقود الورقية أو المعدنية وما يحل محلها من صكوك أو أوراق مالية كالكمبيالات والسند الأذنى في عصر المصارف التقليدية ذات المقرالمحدد مكانيا وقد كان أقصى ما وصلت اليه من تقدم متمثلا في اجراء التحويلات المصرفية بإجراءات ورقية معقدة و مقابل رسوم مالية معينة. فإذا كان الركن المادي للسرقة المتمثل في الاختلاس يمكن ان يطبق على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية فذلك لأن جريمة السرقة من الجرائم ذات القالب الحر لم يحدد المشرع شكل السلوك الإجرامي لها، يمكن أن يتم

[16] عبد الفتاح بيومي حجازي – صراع الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – القاهرة 2007 ص 609

بأي فعل يؤدي الى حرمان المجني عليه من المال المنقول وإدخاله في حيازة الجاني، كذلك الحال بالنسب لجريمة النصب حيث يتحقق السلوك الإجرامي لها بالاستيلاء على أموال الآخر بالطرق الاحتيالية، فهل ينطبق ذلك على جرائم السرقة و الاحتيال التي ترتكب عن طريق التقنة المعلوماتية ؟

لذا سوف نعرض إلى الوسائل الفنية التي يتم عن طريقها الاختلاس قبل أن نعرض تكييفها القانوني في ظل الفراغ التشريعي في ليبيا.

الوسائل الفنية للتحويل الإلكتروني للأموال:

يتم التحويل غير المشروع للأموال بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال لكن يمكن الاشارة إلى أكثرها انتشاراً.

استخدام برامج معده خصيصا لتنفيذ الاختلاس : اشهر هذه الوسائل هو تصميم برامج معينة تهدف الى اجراء عمليات التحويل الالي من حساب الى اخر سواء كان ذلك من المصرف نفسة او من حساب أخر في مصرف اخر على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، واشهر هذه الوقائع قيام احد العاملين بمركز الحاسبات المتعاقد مع مصرف الكويت التجاري لتطوير أنظمة المعلومات بٍالاستيلاء على مبالغ طائلة من المصرف بعد أن تمكن من اختيار خمسة حسابات راكدة في خمس فروع محليه للمصرف واعد لها برنامجا تمثلت مهمته في تحويل مبالغ معينة من هذه الحسابات التي حسابات أخرى فتحت باسمه في الفروع نفسها على أن تتم عملية التحويل

أثناء وجوده بالطائرة في طريقة إلى المملكة المتحدة عائدا إلى بلاده بعد انتهاء عقد عمله، ثم فتح حسابات أخرى فور وصوله وطلب من المصرف تحويل هذه المبالغ إلى حساباته الجديدة في بريطانيا[17]. كما توجد برامج أخرى تقوم بخصم مبالغ ضئيلة من حسابات الفوائد على الودائع المصرفية بإغفال الكسور العشرية بحيث يتحول الفارق مباشرة إلى حساب الجاني لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة ومما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ هو ان هذه الاستقطاعات تتم على مستوى ألاف الأرصدة في وقت واحد مع ضآلة المبلغ المخصوم من كل حساب على حده بحيث يصعب أن ينتبه اليه العميل [18].

2- التحويل المباشر للأرصدة: يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور، أشهرها قيام احد خبراء الحاسب الآلي في الولايات المتحدة باختزاق النظام المعلوماتي لأحد المصارف وقيامه بتحويل 12 مليون دولار الى حسابه الخاص في ثلاث دقائق فقط وعادة ما يتم ذلك ايضا عن طريق ادخال معلومات مزيفة وخلق حسابات و مرتبات وهمية وتحويلها إلى حساب الجاني،ويمكن ان يتم التحويل المباشر ايضا عن طريق

[17] هشام فريد رستم – قانون العقوبات مخاطر المعلومات مكنة الآلات الحديثة أسيوط 1992ص 81

[18]. David Bainbridge- Introduction to computer law-third edition-Pit Man publishing1996 p237

التقاط الاشعاعات الصادرة عن الجهاز اذا كان النظام المعلوماتي متصلا بشبكة تعمل عن طريق الاقمار الصناعية فهناك بعض الانظمة الى تستخدم طابعات سريعة تصدر اثناء تشغيلها اشعاعات اليكترومغناطيسية ثبت أنه من الممكن اعتراضها والتقاطها اثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز واعادة بثها مرة أخرى بعد تحويرها[19]. وهو ما نصت عليه اتفاقية بودابست في المادة 5

3- التلاعب بالبطاقات المالية : لقد ظهرت اولى هذا النوع من الاحتيال بالتقاط الارقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الالي للنقود الى أن ظهرت الصرافة الالية Electronic Banking والنقود المالية digital Cash.

اما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الارقام السرية الخاصة بها وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن ان تسجل عليها أرقام هذه البطاقات. و في هذا النوع من الاعتداءات لا نجد صعوبة في تطبيق نصوص جرائم السرقة والنصب عليها سواء تم ذلك عن طريق سرقة البطاقة نفسها، أو عن طريق سرقة الرقم السري واستخدامه استخدام غير مشروع للتحايل على المؤسسات المالية وصرف هذه المبالغ خاصة أن النموذج

[19] محمد سامي الشوا ثورة المعلومات وبعكسها على قانون العقوبات دار النهضة العربية القاهرة 1994ص 70-72 وما بعدها

التجريمي لجريمة النصب لم يشترط في الوسائل الاحتيالية ان تكون مرتكبة ضد الانسان فيكفي ان ترتكب هذه الوسائل الاحتيالية ضد الآلة ما دامت تؤدي الى الحصول على نفع غير مشروع اضرارا بالاخر من وهو ما نصت عليه المادة 461ع.

جرائم الاعتداء على أجهزة الصرف الآلي للنقود : تثور هذه المشكلة في حالة استخدام الجهاز لصرف ما يتجاوز الرصيد الفعلي اذا تم ذلك بواسطة العميل صاحب البطاقة فالمسألة هنا لا تعدوأن تكون مسألة مديونية بين المؤسسة المالية والعميل ولا يمكن تكييفها بأنها سرقة طبقا للمادة 444ع لان الاستيلاء على المبلغ لم يتم دون رضاء المؤسسة المالية طالما ان هذه الاخيرة تعلم بأن الجهاز غير مرتبط بسقف حساب العميل حتى لا يتجاوزه.

جرائم الاستيلاء على النقود الالكترونية :يمكن تعريف النقود الالكترونية Electronic Cash بأنها "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً، وغير مرتبطة بحساب مصرفي، تحظى بقبول غير من قام بإصدارها، وتستعمل كأداة دفع". وتتمثل أهم عناصرها في أن قيمتها النقدية تشحن على بطاقة بلاستيكية، أو على القرص الصلب للحاسب الشخصي للمستهلك، فهي تختلف عن البطاقات الإئتمانية، لأن النقود الإلكترونية يتم دفعها مسبقاً، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي أنها استحقاق عائم على مؤسسة مالية، يتم بين طرفين هما: العميل والتاجر، دون الحاجة إلى تدخل طرف ثالث،

كمصدر هذه النقود مثلاً 20 فهي مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الالكترونية أن تحل فعليا محل تبادل العملات النقدية(21)، ومن هذه البطاقات ما يعمل عن طريق إدخالها إلى المركز الخاص بالمعاملة المصرفية لدى البائع أو الدائن حيث تم انتقال البيانات الاسمية من البطاقة إلى الجهاز الطرفي للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع[22].

ثالثا: جرائم الإضرار بالبيانات:

يعتبر هذا الفرع من الجرائم الالكترونية من أشدها خطورة و تأثيرا وأكثرها حدوثا وتحقيقاُ للخسائر للإفراد و المؤسسات. ويشمل هذا الفرع كل أنشطة تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة الكترونية Digital) (Formعلى الحواسب الآلية المتصلة أو غير المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غير مشروعة عليها.

[20] محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004، ص142-148.

[21] منير الجنبيهي – ممدوح الجنبيهي – البنوك الالكترونية ط 2 – 2006 دار الفكر الجامعي – الإسكندرية ص47

[22] عبد الفتاح بيومي حجازي – صراع الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – دار للنشر والبرمجيات – القاهرة 2007 ص 609

أبسط تلك الأنشطة هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أى تأثير سلبي عليها. ويقوم بذلك النوع من الأنشطة ما يطلق عليهم المخترقون ذوى القبعات البيضاء (White Hat Hackers) الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الانترنت مستغلين بعض الثغرات فى تلك النظم مخترقين بذلك كل سياسات و إجراءات امن المعلومات التى يقوم بها مديري تلك الأنظمة والشبكات (System And Network Administrators) و كما ذكر عدم ارتباط ذلك النشاط بالشبكات فاختراق الأمن الفيزيقي للاماكن التى يوجد بها أجهزة الحاسب التى تحتوى على بيانات هامة بالرغم من وجود إجراءات أمنية لمنع الوصول إليها و بمعنى أخر وصول شخص غير مصرح له و إمكانية دخوله إلى حجرة الحواسب المركزية بالمؤسسة ثم خروجه دون إحداث أى أضرار فانه يعتبر خرقا لسياسة وإجراءات امن المعلومات بتلك المؤسسة.

استخدام الشبكات و بصفة خاصة شبكة الانترنت فى الدخول على قواعد البيانات أو مواقع الانترنت والحصول على معلومات غير مسموح بها أو إمكانية السيطرة التامة على تلك الأنظمة بالرغم من وجود إجراءات حماية متعددة الدرجات من الحوائط النارية وأنظمة كشف ومنع الاختراق بالإضافة لآليات تشفير البيانات وكلمات السر المعقدة وبتخطي كل تلك الحواجز والدخول على الأنظمة المعلومات ثم الخروج دون إحداث أى تغيير أو

إتلاف بها فانه ابسط أنواع الاختراق الذي يعطى الإشارة الحمراء لمديري النظم وأمن المعلومات بان سياساتهم وإجراءاتهم التنفيذية لأمن المعلومات بحاجة إلى التعديل والتغيير وانه يتعين عليهم البدء مرة أخرى فى عمل اختبار وتحليل للتهديدات ونقاط الضعف الموجودة بأنظمتهم (Risk Assessment) لإعادة بناء النظام الامنى مرة أخرى وأيضا العمل على إجراء ذلك الاختبار بصورة دورية لمواكبة الأساليب الجديدة فى الاختراق. أما بالنسبة الى تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل لنظم المعلومات فان تلك الأنشطة تتم بواسطة أفراد هواه أو محترفون يطلق عليهم المخترقون ذوى القبعات السوداء (Black Hat Hackers)الذين قد يقومون بهذه الأعمال بغرض الاستفادة المادية أو المعنوية من البيانات والمعلومات التى يقومون بالاستيلاء عليها أو بغرض الإضرار بالجهة صاحبة تلك الأنظمة لوجود كره شخصي أو قبلي أو سياسي أو ديني أو القيام بذلك لحساب احد المؤسسات المنافسة.

رابعا جرائم الاعتداء على الأشخاص

المقصود بالاعتداء هنا هو السب و القذف و التشهير و بث أفكار و أخبار من شانها الإضرار الأدبي أو المعنوي بالشخص أو الجهة المقصودة.

هذا و تتنوع طرق الاعتداء بداية من الدخول على الموقع الشخصي للشخص المشهر به وتغيير محتوياته والذى يندرج تحت الجرائم التى تتم ضد الحواسب و الشبكات أو عمل موقع أخر يتم نشر أخبار و معلومات غير صحيحة و

الذي يندرج تحت الجرائم باستخدام الحواسب الآلية و الشبكات والذى غالبا ما يتم من خلال إحدى مواقع الاستضافة المجانية لصفحات الإنترنت و التي أصبح عددها بالآلاف في كافة الدول المتصلة بالإنترنت و التي تسمى بال (Free Web Hosting Services) .

خامسا: جرائم تطوير و نشر الفيروسات:

كانت البداية لتطوير فيروسات الحاسب فى منتصف الثمانينات من القرن الماضي فى باكستان على ايدى اثنين من الإخوة العاملين فى مجال الحواسب الآلية.

استمرت الفيروسات فى التطور و الانتشار حتى بات يظهر ما يقارب المئتين فيروس جديد شهريا. والتي تعددت خصائصها وأضرارها فالبعض ينشط فى تاريخ معين و البعض الأخر يأتي ملتصقا بملفات عادية و عند تشغيلها فان الفيروس ينشط و يبدأ فى العمل الذي يختلف من فيروس لأخر بين أن يقوم بإتلاف الملفات الموجودة على القرص الصلب أو إتلاف القرص الصلب ذاته أو إرسال الملفات الهامة بالبريد الالكتروني و نشرها عبر شبكة الانترنت.

ظهرت مؤخرا نسخ مطورة من الفيروسات تسمى الديدان التى لديها القدرة على العمل والانتشار من حاسب لأخر من خلال شبكات المعلومات بسرعة رهيبة و تقوم بتعطيل عمل الخوادم المركزية والإقلال من كفاءة و سرعة شبكات المعلومات أو إصابتها بالشلل التام .النوع الأخر والذي يدعى حصان طروادة (Trojan Horse) يقوم بالتخفي

داخـل الملفـات العاديـة ويحـدث ثغـرة أمنيـة فى الجهـاز المـصاب تمكـن المخترقـين مـن الدخول بسهولة على ذلك الجهـاز و العبـث بمحتوياتـه و نقـل أو محـو مـا هـو هـام منهـا أو اسـتخدام هويـة هـذا الجهـاز فى الهجـوم عـلى أجهـزة أخـرى فـيما يعـرف ب ال (Leapfrog attack) والـذي يـتم مـن خـلال الحـصول عـلى عنـوان الانترنـت الخـاص بجهـاز الـضحية و منـه يـتم الهجـوم عـلى أجهـزة أخـرى .(IP Spoofing) لا يتصور الكثيرون منا كم الخسائر الناجمة سنويا عن ذلـك النـوع مـن الجـرائم الالكترونيـة ولكن مثال على هـذا مـا جـاء بتعريـف الجريمـة الالكترونيـة سـابقا كيـف ان فـيروس مثـل (WS32.SOBIG)قد كبد الولايات المتحدة أكثر من خمـسين مليـون دولار امـيريكى خـسائر من توقف العمل و فقد الملفات.

سادسا: الجرائم التى تتم باستخدام الحواسب الآلية نظم المعلومات

1جرائم الاعتداء و التشهير و الأضرار بالمصالح الخاصة و العامة:

الاعتداء و التشهير بالأنظمة السياسية و الدينية مستمر و لعل اشهر تلك الوقائع قيام بعض الهواة بوضع بعض البيانات فى شكل صور من القران الكريم و بدءوا فى الإعلان عنها من خلال إحدى مواقع البث المجاني الشهيرة وهو موقع شركة Yahoo و عنوانه (http://www.yahoo.com) الأمر الذي استدعى الأزهر الشريف و المجلس الاعلي للشئون الإسلامية و الكثير من الجهات الإسلامية الأخرى فى شتى بقاع الأرض إلى مخاطبة المسئولين عن الموقع و تم بالفعل إزالة تلك

الصفحات ووضع اعتذار رقيق بدلاً منها.

جرائم الاعتداء على الأشخاص و التى تتم باستخدام الحواسب الآلية و الشبكات قد سبق الإشارة إليها فى الفقرة السابقة و الخاصة بالجرائم التى تتم ضد الحواسب الآلية أما ما يندرج منها تحت بند الجرائم التى تتم باستخدام الحواسب الآلية هو ما يشابه التشهير بالأشخاص المعنويين أو الحقيقيين من بث أفكار و معلومات و أحيانا أخبار و فضائح ملفقة من خلال بناء مواقع على شبكة الانترنت محتويا على كافة البيانات الشخصية مع العديد من الأخبار والموضوعات التى من شأنها الإضرار الادبى و المعنوي و أحيانا المادي بالشخص أو الجهة المقصودة.

يتم أيضا استخدام الحواسب الآلية و شبكة الانترنت فى انتهاك حقوق الملكية الفكرية لبرامج الحاسب و المصنفات الفنية المسموعة و المرئية و نشرها و تداولها عبر شبكات الانترنت فيما يعرف بالقرصنة الأمر الذي يلحق الضرر المادي والمعنوي بالشخص أو الجهة مالكة تلك المواد .و لمكافحة قرصنة برامج الحاسب تقوم منظمة ال بى اس ايه (BSA)العالمية **Business Software Alliance**بتلقي تقارير و بلاغات انتهاكات برامج الحاسب كما تقوم بإنشاء مكاتب لها حول العالم و تقوم بالتنسيق مع الحكومات بالتوعية و محاولة تقليل تلك الجرائم من خلال السعي إلى استصدار قوانين لمعاقبة المخالفين و التى تشير فى تقريرها السنوي الثامن يونيو 2003 إلى أن خسائر شركات البرمجيات وصلت إلى 13.1 مليار دولار اميريكى فى عام

2002 و يشير التقرير أيضا إلى أن أكثر دول العالم فى نسخ البرامج و العمل بنسخ غير مرخصة هى فيتنام حيث يصل نسبة النسخ غير المرخصة إلى حوالي 97 % من إجمالي البرامج المستخدمة يليها دولة الصين بنسبة 94% ثم اندونيسيا بنسبة 89 %. يشير التقرير إلى تحسن نسب القرصنة فى مصر من 86 % عام 1994 إلى حوالي 52% عام 2002.

أما بالنسبة لاستخدام الحاسب لنسخ كافة المصنفات المسموعة و المرئية و توزيعها بصورة غير مشروعة سواء من خلال الاسطوانات الممغنطة او من خلال مواقع الانترنت فان التى انتشرت انتشارا كبيرا فى الآونة الأخيرة وأيضا انتشرت برامج تبادل الملفات بين مستخدمي الانترنت التى يتم استخدامها فى تبادل الاغانى والأفلام و البرامج غير المرخصة. أما فى الولايات المتحدة فقد بدأت رابطة شركات الاسطوانات الاميريكية معركتها ضد المواقع الالكترونية التي تقدم خدمات تبادل الملفات وتحميل الأغاني بالمجاني على أجهزة الكمبيوتر عام 1999 و ذلك بعد انخفاض مبيعات الاسطوانات بنحو 31 % بسبب النقل و النسخ عبر الانترنت و قد تحقق للرابطة بالفعل إغلاق احد اشهر مواقع بث الأغاني والذي يدعى Napster و مازالت العديد من القضايا مرفوعة من قبل الرابطة ضد شركات بث الأغاني أو خوادم التبادل بين المستخدمين بل ووصل الأمر إلى رفع العديد من القضايا على الأطفال والمراهقين مستخدمي تلك البرامج للاستماع و الحفظ و التبادل للمصنفات.

2جرائم الاعتداء على الأموال:

مع زيادة درجة اعتمادية المؤسسات المصرفية والمالية على تكنولوجيا المعلومات و الاتصالات و التحول التدريجي فى كافة أنحاء العالم نحو ما يطلق عليه البنوك والمصارف والمؤسسات المالية الالكترونية، فقد شهد هذا التطور ظهور عدد كبير من الجرائم الالكترونية.

فعلى مستوى البنوك و المؤسسات المالية فقد تم ميكنة نظم الإدارة و المحاسبة و ربط الأفرع المختلفة لتلك المؤسسات بعضها ببعض من خلال شبكات المعلومات لضمان سهولة و يسر إدارة العمليات المالية داخلها. و فى تعامل تلك المؤسسات مع العملاء عن بعد فقد تم تحقيق ذلك عن طريق الاتصال المباشر من خلال شبكات المعلومات الخاصة غير المتاحة لمستخدمي الانترنت (Private Networks) التى كان لها بعض القيود المكانية للاتصال أو من خلال شبكة الانترنت من خلال تواجد واجهة لتلك التعاملات (WebInterface).

تم أيضا دخول بطاقات الائتمان و الدفع الالكتروني (Credit Cards)بأنواعها المختلفة لتسهيل المعاملات و التوجه للإقلال من التعاملات بالنقد المباشر فى إطار التحول إلى المجتمع اللانقدى (Cash-less Society) و بدون الخوض فى تفاصيل فوائد وأهمية مثل هذا النوع من التعامل المالي و آثاره الايجابية على كفاءة البنوك فى القيام بدورها وأيضا آثاره على الاقتصاد ككل. فان ذلك النوع من التعاملات قد أصبح أمرا واقعاً يتزايد الاعتماد

عليه خاصة بعد تنامى حجم الأعمال التى تتم من خلال التجارة الالكترونية (Electronic Commerce)وظهور الأسواق الالكترونية (Electronic Marketplace) لتسويق و بيع السلع والخدمات.

الطبيعة القانونية للجريمة الإلكترونية

يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية حول الوضع القانوني للبرامج والمعلومات، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأية طريقة كانت، لذلك انقسم الفقه اتجاهين : الأول يرى أنه وفقا للقواعد العامة أن الأشياء المادية وحدها هي التي تقبل الحيازة والاستحواذ، وأن الشيء موضوع السرقة يجب أن يكون ماديا أي له كيان مادي ملموس حتى يمكن انتقاله وحيازته عن طريق الاختلاس المكون للركن المادي في جريمة السرقة، ولما كانت المعلومة لها طبيعة معنوية ولا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ، إلا في ضوء حقوق الملكية الفكرية، لذلك تستبعد المعلومات ومجرد الأفكار من مجال السرقة ، ما لم تكن مسجلة على اسطوانة أو شريط، فإذا ما تم سرقة إحدى هاتين الدعامتين الخارجية، فلا تثور مشكلة قانونية في تكييف الواقعة على أنها سرقة مال معلوماتي ذو طبيعة مادية، وإنما المشكلة تثور عندما نكون أمام سرقة مال معلوماتي غير مادي ؛ والاتجاه الثاني يرى المعلومات ما هي إلا مجموعة مستحدثة من القيم

قابلة للاستحواذ مستقلة عن دعامتها المادية، على سند من القول أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة، وأنها ترتبط كما يقول الأستاذان Catala وVivant بمؤلفها عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه، بمعنى أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال [23].

وعلى الصعيد نفسه ثمة من يقول إنه يجب أن نفرق بأن هناك مالاً معلوماتيا ماديّا فقط ولا يمكن أن يخرج عن هذه الطبيعة وهي آلات وأدوات الحاسب الآلي مثل وحدة العرض البصري ووحدة الإدخال، وأن هناك من المال المعلوماتي المادي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية وهي المال المادي الشريط الممغنط أو الاسطوانة الممغنطة أو الذاكرة أو الأسلاك التي تنتقل منها الإشارات من على بعد، كما هو الحال في جرائم التجسس عن بعد، إذن من المنطق القول إذا حدثت سرقة فإنه لا يسرق المال المسجل عليه المعلومة والبرامج لقيمته المادية وهي ثمن الشريط أو ثمن الاسطوانة ، وإنما يسرق ما هو مسجل عليهما من معلومات وبرامج ، ويرى أصحاب هذا الرأي أن التحليل المنطقي يفرض الاعتداد بفكرة الكيان المادي

[23] -- د. محمد على العريان ، المرجع السابق ، ص43 وما بعدها .

للشيء الناتج عنه اختلاس المال المعنوي البرامج والمعلومات، وأنها لا يمكن أن تكون شيئا ملموسا محسوسا، ولكن لهما كيان مادي قابل للانتقال والاستحواذ عليه بتشغيل الجهاز ورؤيتهما على الشاشة مترجما إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي ، وانتقال المعلومات يتم عن طريق انتقال نبضات ورموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل صادرة عنه يمكن سرقته، وبالتالي لها كيان مادي، يمكن الاستحواذ عليه (البرامج والمعلومات)، واستطرد أصحاب هذا الاتجاه في القول بأنه طالما أن موضوع الحيازة (أي المعلومات) غير مادي، فإن واقعية الحيازة تكون من نفس الطبيعة أي غير مادية (ذهنية)، وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر[24].

نظم إدارة حماية المعلومات ISO27001 (المتطلبات)

التطور التاريخي لمواصفة نظم إدارة حماية المعلومات ISO27001

جاءت المواصفة ISO27001 بالاعتماد على المواصفة البريطانية BS7799 والتي كانت نتيجة مبادرة مشتركة من القطاع التجاري والصناعي البريطاني والتي بدأت العمل عام 1992 حيث أصدرت المواصفة البريطانية الأولى BS7799 في شباط عام 1995، حيث مثلت قاعدة ممارسات لإدارة

[24] - د. هدى حامد قشقوش ، مرجع سابق ، ص51-52

حماية تكنولوجيا المعلومات، ثم استمرت المنظمات بتطوير نظام حماية المعلومات التي أفرزت حل سميّ بذلك الوقت (العلاج C) الذي تبنى إطار لتطبيق المعايير الخاصة بحماية المعلومات والتي تم إطلاقها في نيسان عام 1997،لكن بسبب الصعوبات التي واجهتها عملية التطبيق (للعلاج C) تم تنفيذه عام 2000، ذلك بسبب أن BS7799 مرَ بمراجعة هامة عام 1998 والتغذية العكسية رُتبت وتم مراجعتها مرة أخرى وأطلقت النسخة الكاملة الأولى لـ BS7799 عام 1999 كنسخة أصلية لقاعدة الممارسات وحفظت وسميت بـ BS7799 الجزء الأول، أما الجزء الثاني من المواصفة البريطانية BS7799 سميت بـ (المواصفات لأنظمة إدارة حماية المعلومات) والذي يعتبر نظام مقيّم ومصدق وهو موجه لإدارة أنظمة حماية المعلومات. (www.sapphire.net:2007)

ثم مرت المواصفة البريطانية BS7799 بمراجعة أخرى عام 2002 وحصلت على العديد من التغيرات، ثم بقت كما هي حتى تم إصدار المواصفة الدولية ISO27001 في عام 2005 كقاعدة للممارسات والتي تأخذ توجيهاتها ووصياتها من المواصفة الدولية ISO17799:2000 الموازية للمواصفة البريطانية BS7799. (Calder & Watkins,2008,35)

وبهذا يمكن أن تعتبر ISO27001 كقاعدة لتقييم نظام إدارة حماية المعلومات (ISMS) المتكامل، أو هي وثيقة التي تقييم أي نظام لإدارة حماية المعلومات.

عمليات المعالجة ISO27001:2005 وفوائد تطبيقها :

تعد ISO27001 معيار الحماية الدولي الرسمي المقدم لأي منظمة (بغض النظر عن كونها صناعياً كانت أم خدمية) ترغب بالحصول على شهادة مستقلة لنظام إدارة حماية المعلومات الخاصة بهم، لهذا تحدد المواصفة المتطلبات الإلزامية لتأسيس وتطبيق وتوثيق نظام ISMS، وتحديد متطلبات السيطرة لحماية المعلومات التي ستطبق وفق حاجات المنظمة الخاصة بها، وتشمل (11) مركز للسيطرة و (39) هدف للسيطرة بالإضافة الى (133) موقع للسيطرة متوافق مع المواصفة ISO17799 والتي تعمل من خلال أنموذج Plan – Do – Check – Act (PDCA) الذي يقوم بعمل التحسين المستمر، وبهذا تستند المواصفة ISO27001 في عملها على تسعة أجزاء للمعالجة التي حددها تحالف صناعة حماية شبكات الإنترنت * CSIA يمكن تلخيصها بالاتي : (CSIA,2007,3)

تعريف المجال لـنظام إدارة حماية المعلومات ISMS.

تعريف سياسة حماية المعلومات.

تقييم الأخطار /التحليل.

إدارة الخطر.

* Cyber Security Industry Alliance

تحديد الأهداف للسيطرة والسيطرة الفعلية عليها / التطبيق.

تجهيز بيان (كشف) التطبيق.

تطبيق وتشغيل ISMS.

استمرار المراقبة ومراجعة ISMS.

إدامة وتحسين ISMS.

ولانجاز نظام ISMS فعال تستعين منظمة المواصفات الدولية ISO معايير ISO27002 كتعليمات تساعد في تطبيق ISO27001 من خلال الأتي: (Arnason& Willett,2008,8)

تقييم المخاطر والمعالجة.

سياسة الحماية.

تنظيم حماية المعلومات؟

إدارة الموجودات.

حماية معلومات الموارد البشرية.

حماية الطبيعة والبيئة.

إدارة العمليات والاتصالات.

السيطرة على دخول قواعد البيانات.

الحصول على نظم المعلومات، التطوير، الإدامة.

إدارة حوادث لحماية المعلومات.

إدارة استمرارية العمل.

الأبعاد الثلاثة لحماية المعلومات:

يمكن أن تتعرف المنظمة على كيفية إدارة حماية المعلومات من خلال ثلاثة أبعاد (السرية، السلامة، التوفر)

ويمكن توضيح هذه الأبعاد الثلاثة بإيجاز وكالاتي :

السرية Confidentiality : يوفر هذا البعد للمنظمة السرية التامة لكافة المعلومات، حتى لو كانت المعلومات صغيرة وبسيطة.

السلامة Integrity : تقدم المواصفة ISO27001 معيار لحماية وكمال المعلومات وطرائق معالجتها، وهذا يضمن الاستمرارية وإعادة العمل في حالة وقوع الكوارث.

التوفر Availability : ويقصد بالتوفر هو توفر المعلومات المقيد، إذ أن استخدام ISO27001 لحماية نظام المعلومات يؤكد للمنظمة بأن

المستخدمين المخولين هم الوحيدين القادرين على الوصول الى هذه المعلومات وأصولها، وهذا يجعل إدارة حماية المعلومات مهمة سهلة المعالجة.

إدارة دورة حياة المعلومات

طبقا للإحصاءات في بعض المؤسسات الدولية،فان معدل إنتاجية العالم من البيانات والمعلومات الرقمية الناتجة عن استخدام تقانة المعلومات والاتصالات خلال العامين الماضيين قد تجاوز إجمالي ما أنتجته البشرية من معلومات وبيانات طوال تاريخها، إذ أصبحت البيانات والمعلومات في وقتنا الحاضر تتسم بالنمو المضطرد، و تشير الإحصاءات الى إن التزايد في البيانات والمعلومات بنسبة (20%-40%) كمعدل سنوي وهذا يدل على إن العالم يواجه تيارا متدفقا من المعلومات التي تتراكم بسرعة مولدة فيضانا وانفجارا معلوماتياً رقمياً بات من الصعب السيطرة عليه، وإذا كانت هذه القضية لا تعني الكثير بالنسبة للأفراد فهي حيوية ومقلقه وضاغطة للغاية بالنسبة للمنظمات بشكل عام، ذلك بسبب ما يعرف بظاهرة جبال المعلومات والبيانات ألرقميه التي تتراكم وينمو حجمها بمعدلات سريعة, ويصعب إدارتها, وفي الوقت نفسه تحمل المنظمات أموالا طائلة للحفاظ عليها والناجمة عن الاعتماد الكثيف على تكنولوجيا المعلومات في انجاز الأعمال .

ولو عدنا إلى الأساس الفكري والنظري لمفهوم إدارة دورة حياة المعلومات سنجده يهتم بعده نقاط أساسية: (http//:arabinfo.blogsspot.com:4-5)

الأولى: إن إدارة دورة حياة المعلومات ليست تكنولوجيا ولكنها خليط من العمليات والتكنولوجيات التي تحدد كيف تتدفق أو تمر البيانات عبر بيئة ما.

الثانية: إن التكلفة عامل مهم للغاية, لذلك فهو يربط بين الحصول علي قيمه اقتصادية للمعلومات وبين تحمل اقل قدر من التكلفة في إنشاء البنية الأساسية المعلوماتية المطلوبة ليس في مجال تخزين وإدارة المعلومات فقط, ولكن في مراحل المعالجة والنقل والتوزيع وغيرها.

الثالثة: انه يمزج بشكل كامل بين الأهداف التي تضعها المنظمة لنفسها وبين البنية الأساسية المعلوماتية لديها, مما يستدعي ترجمه الأهداف إلى سياسات تنفذ داخل الشبكات والحاسبات وأوعيه التخزين وغيرها من مكونات البنية المعلوماتية.

ويري أصحاب هذا الاتجاه إن النقاط الثلاث السابقة تجعل من المتعين أن يمر التنفيذ العملي لمفهوم إدارة دوره حياه المعلومات بالمراحل التالية:(3: 2004 : wind)

التقييم

والفحص

التهيئة الاجتماعية

التصنيف

الميكنة

المراجعة

تاريخيا البيانات والمعلومات نقلت من وسيلة خزن إلى أخرى، ويتم الاعتماد مبدئيا على عُمر هذه المعلومات أو البيانات، أو عدد مرات الاطلاع عليها أو الدخول عليها. الأقدم أو الأقل استخداما في العادة (على الأرجح) سوف تتحول إلى كلفة قليلة، وأداء منخفض، وأنظمة دخول واستخدام اقل،هذه المشاكل المربكة للمنظمة جعلتها بحاجة إلى المدخل الفوري (immediate access) للمعلومات التي لم تستعمل في اغلب الأحيان،فعلى سبيل المثال السجلات الطبية ربما تكون قديمة، أو إن الدخول والاطلاع عليها قد لا يتم إلا بشكل نادر، بسبب قدمها،لكن في حالات الطوارئ يجب أن تكون هذه المعلومات متاحة في الحال.

يعرف مفهوم إدارة دورة حياة المعلومات على "إنها السياسات والعمليات والممارسات والأدوات المستعملة لترتيب قيمة معلومات وبيانات الأعمال مع البنية التحتية لتقانة المعلومات الأكثر ملائمة،والأقل كلفة في الوقت الذي تعمل به هذه المعلومات مرورا بترتيبها النهائي"وان المعلومات سترتب وترصف طبقا لمتطلبات الأعمال من خلال إدارة السياسات ومستويات الخدمة المرتبطة مع التطبيقات، والحقائق والبيانات.

قواعد إدارة دورة حياة المعلومات في مواجهة التحديات :

أصبح مفهوم دورة حياة المعلومات من المفاهيم العالمية المعاصرة، إذ أن هناك أكثر من (20000) من الأنظمة التي تؤثر على العمليات التي تكون فيها السجلات مخزنة، ويمكن الدخول إليها، ويتم الحفاظ عليها، فضلا عن صيانتها، هذه الأنظمة تحدد حاجة الأعمال للمراقبة المناسبة،وإدارة دورة الحياة الكلية لسجلات المنظمات،وسياسات الأعمال،والعمليات والممارسات،والأنظمة يمكن أن تدقق لغرض الالتزام بالقانون.

إن الحماية (preservation)، والاحتفاظ (retention)، والتطبيع (disposition)، للسجلات الالكترونية سوف تكون باهظة إذا لم تمتلك المنظمة خطة جيدة ومطبقة بشكل ناجح لإدارة دورة حياة المعلومات (www.management1.com:2)

في حالة غياب أي معايير رسمية، فإن منظمات الأعمال تعتبر إدارة دورة حياة المعلومات هي الأسلوب الأفضل لتحسين أداء المنظمات فيما يتعلق بتخزين البيانات والمعلومات، ويجب أن تأخذ هذه المنظمات في الحسبان أن الممارسات الأفضل هي (Thompson, 2005,2)

فهم القيمة الحقيقية بالنسبة للأعمال:

تحديد أي البيانات تشترك بشكل فاعل في الأعمال مقابل تحديد أي البيانات ذات فائدة تاريخية،أو أخذت من الحافظات فقط " just in case "، إذ إن

المستخدمون يحددون البيانات التي خزنت في الحافظات بسبب خشيتهم خسارة الدخول إليها، لذلك فتركيزهم على الاحتفاظ القريب "near-line retention" سوف يساعدهم على تسهيل قراراتهم المتعلقة بهذه الأعمال.

منذ مرحلة التطبيق سوف يتم التطور خلال الوقت، وتضمن بان الحلول القريبة "near-line solution " ستتضمن طبقة بيانات مجردة، لتمكين التطبيق من إزالة أو إضافة أو تعديل أو تكييف عناصر البيانات، بدون أي مهام أدارية رئيسة للبيانات القريبة.

2. توحيد وتبسيط المعايير الجزئية :

اعتبر الوقت كمقياس عند وضع قواعد الأرشفة، معظم الأعمال تجد ذلك الأسهل للفهم والتنفيذ بعد ذلك، ولذلك كثير من عمليات الأعمال نفسها أساسها الوقت ، هذه الإستراتيجية لوحدها ستؤدي إلى تقليل النتائج إلى 50% (أو أكثر تخفيضا من ذلك) في حجم الجزء المخزون على الانترنت.

عند كسب التجربة مع أساليب بسيطة أساسها الوقت

(simple time- based methodology) وبعد ذلك يجب مراعاة القواعد الأساسية لسجلات الاستفسار (query –log) مثل صنف المستعمل (users class) ولم ادخل منذ.... (not accessed since ....).

إستراتيجية النمو المنطقي –إدارة التجزئة

(logical growth – management partitioning strategy)، يمكنها الإبقاء على تفاصيل البيانات القريبة، وتجميع البيانات بشكل فوري مع القدرة على السبر للتفاصيل (drill to to detail).

3. صيانة معمارية التطبيق الأولي:

المعمارية الأولية يجب أن تكون مؤرشفة، وتعيد الخزن بين الأجزاء الفورية والقريبة، وهذا سوف يحافظ على نطاق التطبيق الثنائي المؤسسي المطبق في الوقت الحاضر، ويبسط الإدارة، نموذجيا إعادة الخزن (restore) عملية يمكن أن تؤتمت لمهام موحدة، أو عند الطلب، ونموذج (drill –to –detail) وصف بأنه نموذج مهم،فضلا عن صيانة سلامة التطبيق الحالية.

4.اعتبر الأرشفة غير المتصلة (offline archiving) صفا، إذا أردت الإبقاء على التاريخ التطبيقات مستمرا عدا الخادم الأولي (primary server) للخزن.

إذا حفظ التاريخ لفترات مستمرة،وتم الدخول عليه من قبل المستعملين،وبشكل مستقل لتطبيقات الخزن الأولية (على سبيل المثال التدقيق أو المشاريع الأخرى)

اضمن احتواء ملفات الأرشفة على الحقائق (metadata) فضلا عن البيانات التي يكون لها سياق مستقل عن التطبيق الأصلي. (3-2: 2005: Thompson)**منافع تطبيق إدارة دورة حياة المعلومات:**

إن المنفعة الأساسية من تطبيق إدارة دورة حياة المعلومات هي تعظيم قيمة معلومات الأعمال، فضلا عن تقليل التكلفة الكلية للمالك (total coast of ownership) وتضمن بان البيانات تخزن في مدرج مستوى الخدمات (service-level tier) للحصول على قيمة الأعمال المتأصلة بها،فضلا عن قيمة البيانات سهلة الوصول باستناد إلى حاجات الأعمال في أي مرحلة من مراحل دورة حياتها.بتقليل الزمن المستنفد من قبل الموظفين التقنيين الذين يكونون،ويعالجون هذه البيانات والمعلومات.

إدارة دورة حياة المعلومات تساعد أيضا في زيادة إنتاجية العاملين، وتقليل كلفة العاملين، وفي ذات الوقت، خدمات إدارة دورة حياة المعلومات كأسلوب مفيد للسيطرة على كلفة الانجاز،وإدارة أنظمة الخزن، ومنافع أخرى مشخصة للأعمال ناجمة عن اعتماد أو تنفيذ إدارة دورة حياة المعلومات هي : (Nicolson:2006:80)

الذكاء ألمنظمي (Organizational Agility) ومثال ذلك إيجاد البيانات الصحيحة بصورة أسرع، وتقليل تأثير الأحداث غير المرئية للمنظمة.

تقليل المخاطر مثال ذلك الالتزام ألمنظمي، واستمرارية العمل،الآمن.

يمكن تأشير العديد من المنافع التي يقدمها استخدام مفهوم إدارة دورة حياة المعلومات وذلك من خلال (www.businesssolution.bell.ca:2)

تحسين استخدام المعلومات خلال صفوف الخزن المقسمة.

تبسيط وأتمتة إدارة المعلومات والبنية التحتية للخزن (storage infrastructure)

إعطاء خيارات أكثر ربحا لاستمرارية الدخول إلى الأعمال وحمايتها.

ضمان التزام سهل من خلال سياسات أساسها الإدارة (policy-based management)

تسليم أعلى قيمة في اقل كلفة كلية بترتيب البنية التحتية لعملية الخزن، وإدارة قيمة المعلومات.

الطريق نحو بناء إدارة دورة حياة المعلومات الشاملة:

طور اتحاد الحاسبات إستراتيجية طويلة الأجل والتي لا تُعنى بحاجات إدارة دورة حياة المعلومات اليوم فحسب،لكنها توفر أيضا اتجاها لإدارة المعلومات كموجود بالنسبة للعمل في المستقبل.هذه الإستراتيجية تمكن الزبائن من البدء بوضع الحجر الأساس لإدارة دورة حياة المعلومات الخاصة بهم، وبسرعتهم الخاصة، مع مرونة في اختيار الحلول الصائبة لأعمالهم.

هذه الإستراتيجية تعكس ما نراه كأنموذج نضج لإدارة دورة حياة المعلومات.

المستوى الأول :

إدارة الخزن وحماية البيانات،المنفذة في السنوات السابقة، إذ كانت في السابق لا توجد فعليا كفاءات مؤتمتة، وفي معظم الحالات يوجد جهد بشري عالي،ونموذجيا توجد حالة من التفاعل مع البيئة.

المستوى الثاني :

ويشمل ذلك حلول الخزن الذكية (bright store) فضلا عن منتجات وخدمات من اتحادات الحاسوب والشركاء،وكلها متاحة اليوم، كذلك تزود المنظمة بعرض شامل مع إدارة مصادر الخزن المتكاملة(INTEGRATED STORAGE RESOURCE MANAGEMENT) وإدارة شبكة منطقة الخزن (storage area network management)، وإسناد وإعادة الحلول، هذا سوف يعطي الزبائن المعرفة والفهم والمعلومات المهمة لصنع القرار الصحيح لعمليات الخزن الخاصة بهم.

المستوى الثالث:

إدارة محتويات العمل.والذي يتم التركيز فيه على تعزيز الوثائق،وعمليات التوثيق، وإدارة المحتويات،وأرشفة الرسائل،وهرمية إدارة الخزن (hierarchical storage management)،وخلال هذه المرحلة سوف يتم التخطيط تكامل المنتجات داخل ضمن تنوع أو اختلاف علامة العوائل

لاتحادات الحواسيب العالمية، وتطوير الحلول التي توجه صوب صناعة معينة مثل شركات الأعمال المتوسطة والصغيرة،العناية الصحية،والخدمات المالية.

المستوى الرابع :

توحيد الأعمال ووجهة نظر تقانة المعلومات كرافعة للخدمات الشائعة، والتي هي (البرامجيات،والأجزاء التي تودي الوظائف القابلة للاستعمال مرة أخرى reusable function عبر مجالات الإدارة المتعددة)، وتطوير إدارة قاعدة بيانات مركزية، وإعطاء وجهة نظر وحيدة عن كل سمات المشروع لإدارة المعلومات بشكل عقلاني ذكي، وبشكل امن، وكفوء ولترتيب الموجودات المعرفية تلك مع أهداف العمل.

طرق للحماية من الجرائم الإلكترونية عبر برامج المحادثة الفورية

(Instant Messaging) برامج المحادثة الفورية أو ما تعرف ب الماسينجر، تعتبر أسهل وأسرع طريقة للتواصل على الإنترنت مع الأصدقاء والزملاء، وبالنظر إلى أعداد المسجلين أو المستخدمين لها والذين يفوقون 150مليون شخص في أشهر 4برامج محادثة (AOL. Yahoo. Windows Live Messenger. Jabber) هذا العدد الكبير من المستخدمين وقابليتهم لتشارك الملفات والدردشة، يعتبر مجالا خصبا لخيال واحتيال قراصنة ومجرمي الإنترنت، سواء لتوزيع الديدان أو الفيروسات وأحصنة الطراودة، والاحتيال

كذلك، فهو يمثل بيئة جيدة للاستهداف حيث بالإمكان استعمال منافذ الشبكة المفتوحة من قبل برنامج المحادثة الفورية عوضاً عن فتح منفذ جديد قد يتم غلقه من قبل برنامج الحماية. يكتشف المختصون اليوم طرقاً عديدة لهجمات متعددة ومنوعة من خلال برامج المحادثة الفورية، مستغلين نقاط ضعف المتصفح ونظام التشغيل لتسليم وتوزيع برمجيات خبيثة أو ضارة Malware و Spam وأحصنة طراودة وبرامج تسجيل المفاتيح Keyloggers وسرقة كلمات السر والبيانات الشخصية أو الهامة، وتحويل جهاز الحاسب إلى (زومبي) لتسخيره في هجمات أخرى لصالح المخترق. يستغل الهاكرز أو مجرمو الإنترنت ميزات وسهولة برامج المحادثة الفورية، فهي توفر لهم قائمة كبيرة من الضحايا المحتملين (قائمة الأصدقاء) والإشعار بوقت دخول الشخص الضحية على الشبكة في كل مرة، والمخاطر لا تنتهي هنا فحسب، فمن مزايا برامج المحادثة المهمة: دعم مشاركة الملفات واستخدام Peer-to-Peer مما يسهل عملية إخفاء برمجيات ضارة أو خبيثة داخل الملفات، ويمكن للهاكرز استخدام برامج المحادثة الفورية لإيجاد منفذ خلفي backdoor للأجهزة غير المحمية جيداً، مما يعطيه التحكم والسيطرة الكاملة على الجهاز، فيستطيع تعديل إعدادات النظام ومشاهدة والتصرف بجميع الملفات وكلمات المرور والسجلات، وكذلك استخدام الجهاز ك "زومبي" للهجوم على أجهزة خادمة أخرى مما يتسبب في هجوم "DoS" ما يعرف بحجب الخدمة. الصورة ليست قاتمة تماماً، ولكن لابد من معرفة التهديدات الفعلية والمخاطر المحتملة لاستخدام برامج المحادثة الفورية (الماسينجر) تمهيداً

للبحث حول أفضل الطرق للدفاع والحماية ضد هذه التهديدات والمخاطر، نستطيع إيجازها في عشر طرق أو وسائل للذين يودون إبقاء برنامج المحادثة الفورية (الماسينجر) وسيلة تواصل آمنة وشخصية، سواء لك أو لأفراد عائلتك، وهي: أولاً: لا تستعمل اسمك الحقيقي أو أي معلومات شخصية قد تستغل ضدك، وإذا رغبت في مزيد من الخصوصية والحماية قم بشراء بريد الكتروني مدفوع من احد مزودي الخدمة لاستخدامك الرسمي. ثانياً: لا تعرض اسمك أو بريدك الإلكتروني الشخصي في الأماكن العامة على النت، مثل المنتديات أو الأدلة أو المواقع الاجتماعية، وإذا اضطررت فقم باستخدام بريد الكتروني آخر (ثانوي)، فقد تتعرض لهجمات تصيّد Phishing أو إغراق برسائل Spam ثالثاً: ابق على اتصال مع الذين تعرفهم فقط ويتواجدون لديك في قائمة الأصدقاء، واضبط إعدادات الماسينجر لمنع استقبال الرسائل من أناس لا تعرفهم، وذلك منعاً لاستقبال رسائل سبام عبر الماسينجر IM Spam (Spim). رابعاً: تحاشى ذكر أي معلومات خاصة مثل أرقام الحسابات أو كلمات السر أثناء المحادثة، فقد يتم اعتراضها من قبل برامج التجسس على الشبكة Sniffers، فبرامج الحماية تحمي بياناتك أثناء وجودها في جهازك، وليس أثناء انتقالها خارجه إلى الشبكة. خامساً: حصّن جهازك ببرامج الأمن القوية مع تحديثه باستمرار، وتأكد من احتوائه على مضاد فيروسات ومضاد للسبام والبرمجيات الضارة وجدار نار ومضاد للتصيّد وتقنيات إسناد وتعرّف مبكر للهجمات والملفات الضارة. سادساً: اضبط إعدادات الماسينجر بشكل جيّد، وتأكد من عدم تشغيله آلياً مع بدء

تشغيل الجهاز والنظام، واحرص على إغلاق الجهاز وفصل خط الاتصال سواء كان هاتفيا أو رقميا DSL في حال عدم استخدامك له. سابعاً: حدث نظام التشغيل باستمرار وكذلك برنامج الحماية. ثامناً: لا تفتح أي ملفات أو بريدا إلكترونيا قبل مسحه من برنامج مضاد الفيروسات، ولا تفتح ملفات أو بريدا إلكترونيا من شخص غير معروف، وإذا قمت بذلك فاحذر من فتح الروابط أو الوصلات داخلها. تاسعاً: كن حذراً عند مشاركة الملفات، وارفض تماماً استقبال الملفات ذات الامتدادات (exe..scr..lnk..bat..vbs..dll..bin..cmd.) عاشراً: راقب وحدد طريقة استخدام أطفالك لبرامج الماسينجر، يفضل استخدام برامج المراقبة العائلية لضمان حماية أكبر، وكذلك وضع النظام في نطاق استخدام مرور عائلي مع تحديد وقت الاستخدام الليلي.

حماية أنظمة الدفع المالي

يلقي آخر قسم في هذا الدرس نظرة على خيارات الشركات في تلقي الدفعات على البضائع والخدمات عبر الإنترنت. وهناك العديد من المخاطر في تحقيق أمن وسرية الدفع على الإنترنت.

يعد موضوع السرقة أحد المخاطر الأساسية من منظور المصارف الإلكترونية وشركات البيع بالتجزئة على الإنترنت. وأهم هذه المخاطر هي انتحال هوية

زبون والدخول إلى حسابه المصرفي، وقيامه بشراء البضائع وتسجيلها على حساب ذلك الزبون.

أما من وجهة نظر الزبون، فتتلخص المخاطر بما يلي:

1- سرقة تفاصيل بطاقات اعتمادهم من حواسب ومخدمات الشركة؛

2- قد لا تكون الشركة التي يودون الشراء منها حقيقية.

ولتفادي هذه المشاكل، تقوم الشركات بتطوير أنظمة أمن وحماية مناسبة. وقبل أن نلقي نظرة على المبادئ التي تستند إليها هذه الأنظمة، علينا مراجعة المصطلحات العامة لمختلف الأطراف المشاركة في هذه الإجرءات:

- المشتري: هو الزبون الذي يقوم بشراء البضاعة أو المنتج أو الخدمة؛

- التاجر: هو بائع التجزئة؛

- شهادة الوثوقية (Certification Authority (CA: هي الجهة التي تصدر الشهادات الرقمية التي تثبت هوية كل من التاجر والمشتري؛

- المصارف: هي المصارف التقليدية؛

- مصدّر العملة الإلكترونية: هو مصرف افتراضي يقوم بإصدار عملة رقمية.

إن المتطلبات الأساسية للأطراف المذكورة لأنظمة الحماية الخاصة بالإجرائية المتبعة هي كما يلي:

1- الوثوقية: هل تم التأكد من هوية الأطراف المشتركة بالعملية التجارية؟

2- السرية والخصوصية: هل تمت حماية معطيات العملية التجارية؟ وماهي الإجراءات اللازمة في حال رغب المستهلك بأن يقوم بالشراء تحت اسم مغفل؟ هل يتم نقل جميع المعطيات الغير ضرورية للعملية التجارية من الشبكة العامة وهل يتم حذف السجلات المؤقتة من النظام؟ هل يمكن التجسس على هذه العملية؟

3- التأكد: ماهي إجراءات التحقق من وصول الإرسال بدون تحريف أو تبديل؟

4- عدم الإنكار: كيفية ضمان أن المرسل غير قادر على إنكار قيامه بإرسال رسالة معينة؟

5- الاستمرارية: كيف يمكن إزالة التهديدات التي تواجه استمرار عمل النظام وأداؤه؟

التواقيع الرقمية Digital Signatures

هي طريقة لتحديد هوية الأفراد والشركات من خلال التشفير بالمفتاح المعلن.

يمكن استخدام التواقيع الالكترونية لبناء نظام آمن باستخدام مايعرف بالتشفير بالمفتاح المعلن لتحقيق الوثوقية، أي أن كلاً من التاجر والمشتري حقيقي وغير مزيف. يتم تشفير توقيع الشاري الرقمي قبل إرسال الرسالة باستخدام مفتاحه الخاص، وعند الاستقبال، يتم استخدام المفتاح المعلن للشاري لفك تشفير ذلك التوقيع. وبهذا، يمكن إثبات هوية الزبون. إلا أن التواقيع الالكترونية لاتستخدم على نطاق واسع بسبب صعوبة إعداد المعاملات التجارية حالياً، ولكنها ستنتشر بشكل أوسع مع استقرار البنية التحتية لنظم المفتاح المعلن أو PKI، ومع تزايد استخدام شهادات الوثوقية.

التشفير بالمفتاح المعلن Public Key Encryption

يمكن للزبون باستخدام هذه التقنية أن يقوم بطلب شراء من شركة بالبحث عن المفتاح المعلن لهذه الشركة المتوافر على الإنترنت، ويتم استخدام هذا المفتاح لتشفير الرسالة الحاوية لهذا الطلب. وعندما يتم ارسال الرسالة المشفرة عبر الإنترنت، تقوم الشركة باستلامها ومن ثم قراءتها باستعمال مفتاحهم الخاص. وبهذه الطريقة لا يستطيع أحد باستثناء الشركة الإطلاع على الطلب. وبالعكس، تقوم الشركة بالتأكد من هوية الزبون بقراءة معلومات الهوية، مثل التوقيع الإلكتروني المشفر بمفتاح الزبون الخاص، وذلك باستخدام مفتاح الشركة المعلن.

ولكي تكون نظم التواقيع الالكترونية والتشفير بالمفتاح المعلن فعّالة بالنسبة للشركات والمستهلكين، لابد من التأكد بأن المفتاح المعلن الذي يُنوى استعماله لفك تشفير وثيقة ما ينتمي حقاً للشخص الذي قام بإرسال تلك الوثيقة. والحل الأمثل لهذه المشكلة، والذي لا يزال قيد التطوير، هو أن يتولى طرف ثالث موثوق أو TTP: Trusted Third Party مسؤولية ضمان احتواء الرسالة لمعلومات هوية المالك، ونسخة من المفتاح المعلن الخاص بذلك المالك. ويشار إلى TTP عادةً بإسم مصدر شهادات الوثوقية CA، وستقوم جهات متعددة كالمصارف ومكاتب البريد غالباً بالقيام بهذا الدور في المستقبل.

ما هو الحل العملي إذاً بالنسبة للتجارة الإلكترونية؟ الحقيقة هي أن معظم صفقات ومعاملات التجارة الإلكترونية لاتستخدم التواقيع الالكترونية في الوقت الحالي.

بروتوكول طبقة المداخل الآمنة (Secure Sockets Layer - SSL)

يعد بروتوكول طبقة المداخل الآمنة SSL هو بروتوكول أمني قامت شركة Netscape بتطويره ودمجه في مستعرضها Navigator. اليوم، تدعم جميع المستعرضات الأخرى بما في ذلك مستعرض مايكروسوفت Internet Explorer هذا البروتوكول. إلا أن هناك برتوكولاً جديداً يعرف بإسم بروتوكول طبقة النقل الآمنة TLS أو Transport Layer Security.

ويستخدم بروتوكول SSL في معظم معاملات التجارة الإلكترونية وخاصة تلك المتعلقة بـB2C ، بما في ذلك إجراءات بطاقات الاعتماد، حيث أنه من السهل على الزبون أن يستخدم هذا البروتوكول دون الحاجة لتنزيل برمجيات إضافية أو شهادات رقمية. أما الشركة فتكون موثوقة لإن شهادة مفتاحها المعلن تكون مصدّرة من شركة معتمدة مثل مثل Verisign. وهذا يعني أنه بمقدور الشاري أن يثق بهوية هذه الشركة، بينما لاتستطيع الشركة التأكد من هوية الزبون. يتم استخدام بروتوكول SSL لحظة دخول الزبون إلى موقع تجارة الكترونية، ويقوم النظام بإعلام الزبون بأنه على وشك أن يتلقى معلومات عبر اتصال آمن، ويستخدم رمز مفتاح للإشارة إلى أمان الإجراء. وعندما تستخدم تقنيات التشفير، تتغير بادئة عنوان موقع الويب في المستعرض منhttp:// إلى [ندعوك للتسجيل في المنتدى أو التعريف بنفسك لمعاينة هذا الرابط] ويظهر رمز قفل في أسفل نافذة المستعرض.

بروتوكول المعاملات الإلكترونية الآمنة

(Secure Electronic Transactions -SET

يعد بروتوكول المعاملات الالكترونية الآمنة SET من أكثر البروتوكولات أمناً لأنه يعتمد على الشهادات الرقمية التي طورها الإتحاد الذي تديره كل من شركتي Mastercard و Visa المصدريين الرئيسيين لبطاقات الاعتماد في العالم. ويسمح هذه البروتوكول للأطراف المشاركة بالشراء والبيع التأكد من

هوية بعضهم البعض. وباستعمال الشهادات الرقمية، يسمح بروتوكول SET للشاري بالتأكد من شرعية الشركة، وبالمقابل يعطي الشركة الفرصة للتأكد من أن بطاقة الإعتماد تُستخدم بالفعل من قبل مالكها الحقيقي، وهذا هو الاختلاف الرئيسي عن SSL. إضافة، فإن بروتوكول SET يشترط وجود توقيع إلكتروني في كل طلب شراء لزيادة تأكيد هوية المشتري للبائع، فوجود التوقيع الإلكتروني وشهادة البائع الرقمية يؤمن مستوى أكبر من الثقة.

وعلى الرغم من أن إطلاقه كان في أواخر التسعينات، إلا أن بروتوكول SET لم ينتشر بصورة واسعة بسبب صعوبة تبادل المفاتيح، حيث يحتاج الزبون للحصول على مفتاحه أن يقوم بتركيب مجموعة برمجيات أمان، مثل Microsoft Wallet على نفس الحاسب الذي يحتوي على مفتاحه الخاص. أخيراً، تعد إجراءات SET للتأكد من المعاملات أبطأ من SSL، وعلى الشركة أن تستخدم برمجيات SET خاصة على مخدمهم.

الدفعات الإلكترونية الصغيرة Micropayments

شهدت التسعينات عدة محاولات لتطوير نظم دفع بديلة لبطاقات الإعتماد. وركّزت هذه النظم على الدفعات الإلكترونية أو القطع النقدية الإلكترونية، وخاصة للعمليات التجارية الصغيرة، حيث أن أجر استخدام بطاقة اعتماد لتنزيل جريدة من الإنترنت، مثلاً، غير مجد اقتصادياً لأنه يكلف أكثر من ثمن الجريدة.

وقد فشلت العديد من المبادرات التي قامت بها شركتي Digicash و eCash لأنها لم تحظ بقبول كبير، في حين كانت بطاقات الإعتماد تستخدم بشكل أوسع ولدفعات أكبر، ولم تكن هناك أية حاجة ملحة للدفعات الصغيرة حينذاك. ولكن على الرغم من ذلك، أصبحت بعض الأنظمة البديلة مثل Paypal ([ندعوك للتسجيل في المنتدى أو التعريف بنفسك لمعاينة هذا الرابط] ذات شعبية كبيرة، الأمر الذي مكّن الشركات الصغيرة والأفراد الذين لايستطيعون تحمل كلفة استخدام بطاقات الاعتماد من قبول الدفعات على الإنترنت. فمثلاً، يستخدم زبائن eBay هذا النظام على نطاق واسع.

المعاملات بين الشركات Business-to-Business Transactions

أسست شركة "طاولة الشراء المستديرة عبر الإنترنت" منظمة اسمتها: "الشراء المفتوح على الإنترنت" OBI وموقعها: [ندعوك للتسجيل في المنتدى أو التعريف بنفسك لمعاينة هذا الرابط] وذلك بهدف ضمان إمكانية الاتصال بين أنظمة التجارة الإلكترونية المختلفة، وقد دعمتها شركات كبيرة، مثل: M3 و Ford و Visa و Mastercard و Microsoft. تحدد معايير OBI الخطوات المحددة في إجرءات البيع الحالية، وتوفر عناصر اتصالات موحدة بحيث يستطيع كل من البائع والمشتري القيام بمعاملات معقدة تتطلبها تجارة الشركاتB2B الإلكترونية.

فيما يلي تعداد للإجراءات التي تحددها مقاييس OBI:

1- استمارة الطلب

2- أمر الشراء

3- تأكيد استلام أمر الشراء

4- إعلام مسبق بالشحن

5- وضعية الطلب

6- الفاتورة: سير المعاملة

7- طريقة الدفع: قيد التنفيذ

التحويلات المالية الرقمية أو الإلكترونية EFT (Electronic or Digital Funds Transfer)

يتم استخدام التحويلات المالية الإلكترونية EFT لنقل الأموال مباشرة من مصرف لآخر دون أي حاجة لاستخدام النقود التقليدية. بعض الأمثلة عن عمليات التحويلات المالية الإلكترونية: شركة Direct Deposit البريطانية وموقعها على الإنترنت: [ندعوك للتسجيل في المنتدى أو التعريف بنفسك لمعاينة هذا الرابط] وشركة BACS البريطانية أيضاً: [ندعوك للتسجيل في المنتدى أو التعريف بنفسك لمعاينة هذا الرابط] التي تقوم بإيداع رواتب

الموظفين المستحقة مباشرة في حساباتهم المصرفية. بأية حال، تشير التحويلات المالية الإلكترونية على عملية نقل الأموال التي تتم عبر جهاز الكتروني، ويشمل هذا تحويلات بطاقات الاعتماد.

تبادل المعطيات الإلكترونية EDI على الشبكات الخاصة وعلى الإنترنت

يعود تاريخ التجارة الالكترونية إلى ماقبل الحواسب الشخصية والشبكة العنكبوتية العالمية بهامش بسيط. ففي الستينات، أصبح تبادل المعطيات الالكترونية عبر الشبكات الخاصة الآمنة داخل الشركات وبين المؤسسات صيغة راسخة للتعاملات التجارية. وتعود فكرة مقاييس تبادل الوثائق إلى جسر برلين الجوي في عام 1948، حيث تطلب الأمر وجود قوائم موحدة لإدارة حركة الطيران القادم إلى برلين من مواقع مختلفة بشكل فعّال. وقد قامت وزارة التجارة والصناعة البريطانية بتعريف EDI على الشكل التالي:

"إن تبادل المعطيات الالكترونية EDI هو تبادل المعطيات المنظمة من حاسب إلى حاسب، وإرسالها ومعالجتها بطريقة مؤتمتة، بدون أي تدخل يدوي، عبر شبكاتEDI خاصة في معظم الأحيان."

ويشير تقرير شركة IDCالعام 1999 أن عائدات التبادل الإلكتروني للمعطيات وخدمات EDI المصرفية بلغت حوالي 1,1 مليار دولار في ذلك العام، وأنها تتوقع أن هذه العائدات ستتجاوز ملياري دولار في عام 2003. إن تبادل المعطيات الإلكترونية يتطور من خلال معايير حديثة ومن خلال

تكامله مع تقنيات الإنترنت لتحقيق عمليات EDI على الإنترنت. ويتنبأ التقرير بأن حصة EDI على الإنترنت من العائدات الكلية لـ EDI ستقفز من 12% إلى 41% خلال نفس الفترة. إن حجم تبادل المعطيات الإلكترونية على الإنترنت يتزايد بسرعة كبيرة، بينما ستضمن تعديلات مقاييس EDI المقترحة من قبل "فريق XML EDI" وموقعه: [ندعوك للتسجيل في المنتدى أو التعريف بنفسك لمعاينة هذا الرابط] استمرارية هذا التبادل في المستقبل. ويعد استخدام XML في معاملات B2B مثل CommerceOne و Biznet التابعة لشركة مايكروسوفت توسعاً ملحوظاً في عمليات تبادل المعطيات الإلكترونية.

تبادل المعطيات الإلكترونية EDI على الإنترنت

بعض استخدامات معطيات EDI بواسطة شبكات IP غير خاصة.

تبادل المعطيات الإلكترونية EDI في القطاع المالي

إن أحد أشكال EDI هي آلية الدفع الإلكتروني المتضمن نقل العائدات المالية من مصرف الشاري إلى البائع.

الشبكات المضافة الافتراضية (VAN (Virtual Added Networks

هي شبكات آمنة متباعدة جغرافياً تستخدم تقنية خاصة عوضاً عن تقنية الإنترنت.

الشبكات الخاصة الافتراضية (VPN (Virtual Private Networks

وهي شبكات افتراضية تؤمن اتصال آمن مشفر بين نقطتين بوساطة الإنترنت، يتم إعدادها عن طريق مزودي خدمة الإنترنت ISPs للشركات الراغبة بالقيام بعمليات تجارية آمنة عن طريق الإنترنت.

الجرائم الإرهابية التقنية وطرق مواجهتها:

لقد زادت في الآونة الأخيرة الجريمة، بشكل يصعب معه تحديد مرتكبيها ومعاقبتهم، وذلك نظراً لاستخدام أساليب التقنية رقمية، جعلت من الصعوبة بمكان الوصول إلى المجرم في ظل هذا النظام التقني والفضائي الحديث.

وهذه مشكلة كبيرة يعاني منها كل من الدول المتقدمة تكنولوجياً، والدول النامية التي تأخذ ببعض البرامج التكنولوجية الحديثة. وذلك بسبب تعدد الأساليب المتعلقة بالجريمة التقنية من ناحية، ونوعية المجرم التقني الذي يستخدم هذه الأساليب التقنية الرقمية من ناحية أخرى. لذلك لابد لنا أن نتعرف على الأساليب الإلكترونية الرقمية، ونوعية المجرم التقني الرقمي، وكذلك أنواع تلك الأساليب التقنية المستخدمة في هذه النوعية من الجرائم.

فإذا ما تم لنا معرفة ذلك، أمكن لنا أن نشكل الأساليب المضادة للحد من الجريمة وضبطها، وبذلك تسهم هذه المعرفة في تمكن رجال البحث الجنائي

الإلكتروني من ضبطها، حتى تكون معرفتهم لهذه الجرائم التقنية الرقمية سابقة على المجرم الإلكتروني الرقمي في الوقت الراهن.

وقد تعددت، بل واختلفت طرق وأساليب جرائم الحاسبات الآلية والإنترنت، فهناك أساليب شائعة ومعروفة في ارتكاب جريمة الحاسب الآلي، والتي يمكن أن توظيف في مجالات الإرهاب المتنوعة والمتعددة، نذكر منها على سبيل المثال لا الحصر ما يلي (مصطفى موسى، 2005، 144 – 220):

أولاً: الأساليب الإجرامية الإلكترونية في الاعتداء على المال، ويتضمن المزادات الإجرامية عبر الإنترنت، التسول عبر الإنترنت، الاستيلاء على بطاقات الائتمان، أساليب التحويل الإجرامية بالتقنية الرقمية.

ثانياً الأساليب الإجرامية الإلكترونية الرقمية في الاعتداء على العرض والنفس والتي تتضمن الدردشة المثيرة للغريزة، وإنشاء مواقع إباحية، وإرسال رسائل الكترونية إباحية، وإنشاء مواقع لممارسة الجنس عبر الإنترنت ويمكن أن نستخدم تلك الأساليب عبر الإرهابيين للابتزاز والحصول على مال أو معلومات يمكن أن توظيف في أي عمل إرهابي.

ثالثاً: الأساليب الإجرامية الإلكترونية الرقمية المضرة بأمن المجتمع ومنها أساليب منع الوصول إلى المواقع عبر الإنترنت من خلال إغراق المواقع المستهدفة بمجموعة من البيانات تفوق الجيجا بايت في الثانية الواحدة وتلك البيانات عبارة عن طلبات غير حقيقية.

كذلك التهديد عبر الإنترنت، نشر العنصرية وإذكاء التمييز العنصري، التزوير الإلكتروني الرقمي للأوراق المالية.

وقد أخذت كثير من الدول والمجتمعات حالياً بنظام الإدانة الإلكترونية أو الحكومة الإلكترونية في كثير من تعاملاتها ونظمها ومن المفيد في هذا الصدد:

أولاً: تزوير البيانات والمعلومات أو المخرجات الكومبيوترية الخاصة بالحكومة الإلكترونية:

ثانياً: جرائم الأموال: مثل سرقة المعلومات المالية والأموال، واختراق الحسابات المصرفية وتحويل مبالغ مالية من حسابات العملاء إلى حسابات المخترقين وجريمة الإتلاف المعلوماتي.

ثالثاً: جرائم الاعتداء على بيانات الحكومة الإلكترونية: والركن المادي لهذه الجريمة له صور متعددة منها الدخول غير المشروع لمواقع الحكومة الإلكترونية والتعدي على البيانات الشخصية، وانتهاك سرية وخصوصية البيانات، والاعتداء على التوقيع الإلكتروني والاعتداء على البيانات المشفرة.

لذلك، فإن الأسلوب الإجرامي، هو ذلك الذي يتعلق بكيفية قيام المجرم باستخدام طريقة تتصل بالفعل أو الأداء المتمثل في القيام بفعل أو الامتناع عنه مما يحدث اضطراباً في المجتمع نتيجة مخالفة قواعد الضبط الاجتماعي.

وهذا الفعل أو الامتناع، يطلق عليه اسم "الجريمة" وعلى من أرتكبه اسم "المجرم" والفعل الذي يرتكبه المجرم بواسطة وسائل تقنية الكترونية رقمية سواء شبكة الإنترنت أم بدونها، يمكن أن يطلق عليه اسم "الجريمة الإلكترونية" ويطلق على من يرتكبها اسم "المجرم الإلكتروني الرقمي" وعندما نقول أساليب الجريمة الإلكترونية، فإننا نقصد هنا بالأساليب الإجرامية الرقمية، كيفية استخدام الحاسب الآلي بنظمه، وبرامجه، ووسائل الاتصال الرقمي، في ارتكاب الجرائم، سواء كانت هذه التقنية الرقمية هي محل الجريمة أم كانت وسيلة من وسائل ارتكابها، وسواء كانت عبر شبكة الإنترنت أو بأي أسلوب تقني أخرى، يستخدم وسائل الكترونية رقمية حديثة.

ويستخدم "الإنترنت كوسيلة لارتكاب الجرائم والتي تنقسم إلى قسمين:

الأول: وهو القسم الذي يحمل طابعاً جنائياً بحتاً.

والثاني: وهو يحمل طابع سياسي.

وسواء كانت الجرائم التي ترتكب تحمل طابعاً جنائياً بحتاً، أو طابعاً سياسياً خالصاً، وهي جرائم تبدو تقليدية تماماً، فإن الوسائل التي تستخدم في ارتكابها اليوم، تعد وسائل تقنية والكترونية رقمية، وخاصة أن الوسيلة التي تستخدم في ارتكابها هي "الإنترنت" مما يجعلها تصبح جريمة الكترونية رقمية ذات طابع تقني في أسلوبها وفي طريقة القيام بها.

توجيهات عملية في ضبط وتفتيش انظمة الكمبيوتر والشبكات

ثمة في هذا المقام بعض التوجيهات، لكنها ليست ذات قيمة دون التدخل التشريعي لافراد قواعد تفتيش وضبط خاصة على نحو ما قررته التشريعات الوطنية المقارنة والوثائق الدولية.

ان القاعدة الاولى ان التفتيش يتطلب مذكرة قضائية تجيز تفتيش أنظمة الكمبيوتر. واما اجراء التفتيش دون مذكرة قضائية او الحصول على بيانات من جهات ليست محلا للاشتباه لتعلقها بالمشتبه به، فانها مسائل تثير الكثير من المعارضة خاصة في ظل ما تقرر من قواعد تحمي الخصوصية وتحمي حقوق الافراد وتوجب مشروعية الدليل وسلامة مصدره، او تبطل كل اجراء يتم خلافا للقواعد الاصولية المتعلقة بالتفتيش والضبط المنصوص عليها في القانون ، وهي مسائل – طبعا تختلف احكامها باختلاف النظم القانونية - ينفد من خلالها الجناة عند عدم اجازة القانون هذا المسلك الاستثنائي وعلى نحو يجعلنا متمسكين بضرورة عدم اللجوء الى هذا السلوك – حتى لو اتاح النظام القانوني المعني ذلك مع تحفظنا على مثل هذا الحكم لان المشروعية الاجرائية توجب تحقيق اقصى ضمانات للمتهم تتفق ومقتضيات قرينة البراءة – ونرى الاصرار على وجوب استصدار مذكرات التفتيش، اما مشكلات التفتيش فان حلها وتجاوزها امر منوط بالقواعد القانونية المتعين سنها اضافة الى التزام جهات التفتيش الحيطة في توفير متطلبات القانون والحيطة في مراعاة

بعض المسائل الفنية في هذا الشان – نورد بعضها تاليا - واخيرا أهمية مباشرته ممن تتوفر لديهم الخبرات الفنية الكفيلة بتحقيق التفتيش غرضه.

فاذا كان المحقق يعلم ابتداءا عن وجود الادلة المتصلة بجريمة ما ضمن احد انظمة الكمبيوتر او الشبكات، وكان الجرم ابتداءا من طبيعة الجرائم الالكترونية، فان مذكرة التفتيش يتعين ان تكون واضحة في تحديد النظام محل التفتيش وايراد اوسع وصف يغطي ما يعرفه المحقق سلفا وما يفترض انه يتصل بالمسائل التي يعرفها.

اما ان كان النظام او مكان وجود الدليل غير معروف في نطاق المكان محل التفتيش فيتعين ان تجيء عبارات مذكرة التفتيش عامة ما امكن حتى لا يكون نصها قيدا على نطاق التفتيش والضبط، فعلى سبيل المثال يمكن ان تتضمن مذكرة التفتيش والضبط ((اجراء التفتيش والضبط لاي من او لكل سجل او معلومات توجد بصورة الكترونية او مادية او خطية موجودة في اي جهاز لتخزين المعطيات سواءا كان نظام كمبيوتر ايا كان وصفه او شبكة معلومات او وسائط تخزين او اجهزة اتصال او اية نظم معالجة وتخزين يمكن ان يوجد فيها الدليل)) لكن عمومية مذكرة التفتيش لا تعني عدم وجوب بيان السبب ومبرر التفتيش، ولا تعني تجاوز الاجراء بذاته للقواعد القانونية المقررة لحماية الافراد، خاصة اؤلئك الذين لا صلة مباشرة لهم بالمشتبه به او بفعله.

ومن حيث الاصل فان التحري والتفتيش في بيئة جرائم الكمبيوتر والانترنت يتوقف على مدى دقة مذكرة التفتيش ونطاقها المكاني، ويتعين ان يحرص المحققون او جهات الضبط المكلفة بالتفتيش من قبل النيابة على ان تغطي مذكراتهم اي مكان توجد فيه هذه البينات الالكترونية في نطاق الاختصاص المكاني وبالنظر الى الشخص او الجهة التي يدور التفتيش بشأنها. وهنا تظهر اهم مشكلة في مسائل التفتيش بالنسبة الى اختراقات الانترنت او الاختراقات الخارجية، اذ قد يتطلب التحري تفتيش انظمة كمبيوتر عائدة لجهات لا صلة لها بالفعل او نتيجته، كتفتيش نظم مزودي خدمات الانترنت، او تفتيش انظمة الخوادم خارج الحدود او الطلب من مالكيها ومديريها تزويد جهة التحقيق ببيانات معينة، ولا يمكن ان يقبل قانونا ان تغطي مذكرات التفتيش مواطن ومواقع واماكن خارج صلاحية نظام العدالة المكانية، ومن هنا نشات الحاجة الى تعاون دولي حقيقي في ميدان انشطة التحري والتحقيق والضبط والتفتيش خارج الحدود.

اما مسالة حاجة انشطة التفتيش للسرعة ومسالة قدرة الجناة على اخفاء الدليل فهي التي استوجبت التفكير بآلية استصدار اوامر الحفظ المستعجلة للجهات التي قد تتوفر لديها البيانات المرتبطة بنشاط المشتبه به (هذا بالنسبة للغير)، ومعلوم انه لا يمكن الزام اية جهة بتقديم اية بيانات بشان الخدمات المقدمة للزبائن او علاقتهم به، لان هذه البيانات في الاصل سرية ولا يجوز افشاؤها الا وفق القانون، فان الحاجة تعدو ماسة للتدخل التشريعي لاتاحة

مكنة وايضا آلية الضبط المستعجل للنظم المشتبه بها مع امر كف يد المشتبه به عن استخدام النظام فورا بمجرد البدء باجراءات التفتيش، اضافة الى الحق في ضبط الاجهزة لاجراء التفتيش عليها في مقار التحقيق باستخدام التقنيات التي تتيح ذلك والتي قد لا تتوفر في مكان التفتيش، خاصة اذا ما علمنا ان تفتيش جزء صغير جدا من الذاكرة قد يحتاج ساعات، فكيف هو الحال وقد اصبحت ذاكرات الكمبيوترات قادرة على تخزين ملايين الملفات، اضافة الى ان التفتيش الاولي قد لا يحل مشكلة الملفات المخباة او المحمية او المشفرة. لكن هذه الحلول في نطاق التفتيش تناقض القواعد المقررة قانونا في حقل ضمانات المتهم (اي المتهم المعلوماتي في حالتنا) وضمانات احترام حقوق الانسان والحريات الفردية وفي مقدمتها الخصوصية. فمثل هذه الاجراءات قد تؤدي الى كشف بيانات شخصية او كشف اسرار العمل او الوصول الى ملفات يحرص اصحابها على سريتها او تيح لهم القانون ذلك، وتعدو المسالة اكثر خطورة عندما يمتد التفتيش الى نظم مرتبطة بالنظام موضوع الاشتباه، فتطال ملفات وبيانات جهات لا علاقة لها بالجريمة قد تكون خاضعة لسرية مهنية او قواعد حماية سرية بيانات العملاء كما في حالة نظم الكمبيوتر الخاصة بمزودي الخدمات او نظم كمبيوترات البنوك او الجهات الصحية او اعمال المحاماة او غيرها.

ان الحاجة الى التنظيم التشريعي لجوانب الضبط والتفتيش في حقل جرائم الكمبيوتر ومسائل حماية البيانات الشخصية ايضا، تجد موجبها في الحاجة الى

توفير معيار مقبول يقيم توازنا بين حقوق وحريات الافراد وحماية خصوصياتهم، وبين موجبات المكافحة وحاجتها الى قواعد استثنائية فرضتها تحديات هذه الجرائم التي تزيد عن تحديات غيرها.

ففي ظل سرعة اتلاف الدليل وطبيعة ما يثبت الجريمة ذاتها من الادلة، وفي ظل الحاجة للتدخل السريع لضبط متعلقات الجريمة، وفي ظل ارتباط مادة الجريمة او وسيلتها بانظمة اطراف اخرى لا صلة لهم بها او بشبكات ونظم معلومات خارج الحدود، فان المكافحة الفاعلة قد تنطوي على اهدار لحقوق وحريات الكثيرين والتفريط بضمانات المتهم وما توجبه قرينة البراءة المقررة له، وهذا التناقض لا مجال لفضه الا باقامة معيار تعكسه القواعد التشريعية، فالاستثناء على الحرية والقيد المقرر عليها يعدو مقبولا في ضوء اعتبارات مصلحة المجتمع وامنه متى ما توفر بحق هذا المبرر ومتى ما كان المعيار مدركا ان الاستثناء لا يجوز التوسع فيه ويتعين تقييده بالقيد التشريعي الواضح الذي لا يتيح للسلطات التغول بما منحها القانون من حقوق او بما تفسره هي وفق رؤيتها لما قرره القانون لها من صلاحيات.

طرق مكافحة الإرهاب الإلكتروني

إن المخاطر الكامنة في تغلغل تقنية المعلومات الحديثة في واقعنا تتطلب من المجتمع والدول جميعًا الحيلولة دون حصول تلك المخاطر بشتى أنواعها، ومن أهم ما يجب توفيره في هذا الصدد الأحكام والأنظمة واللوائح المنظمة لسلوك

الأفراد والمؤسسات حيال التعامل مع تقنية المعلومات مهما كان نوع التعامل وأيًا كانت مقاصده، دون تقييد لحرية المجتمع عن الاستثمار البناء لتلك التقنية.

إنه وبالرغم من إدراك أهمية وجود وتطبيق أحكام وأنظمة لضبط التعاملات الإلكترونية فإن الجهود المبذولة لدراسة وتنظيم ومتابعة الالتزام بتلك الأحكام لا يزال في مراحله الأولية، وما تم في هذا الشأن لا يتجاوز مجموعة من القرارات المنفصلة واللوائح الجزئية التي لا تستوعب القضايا المستجدة في أعمال تقنية المعلومات، كما لا توجد بصورة منظمة ومعلنة أقسام أمنية، ومحاكم مختصة، ومنتجات إعلامية لشرائح المجتمع المختلفة [25].

أنظمة الحماية الفنية من الاعتداءات الإلكترونية

منذ أول حالة لجريمة موثقة ارتكبت عام 1958م في الولايات المتحدة الأمريكية بواسطة الحاسب الآلي وحتى الآن كبر حجم هذه الجرائم وتنوعت أساليبها وتعددت اتجاهاتها وزادت خسائرها وأخطارها، حتى صارت من مصادر التهديد البالغة للأمن القومي للدول، خصوصًا تلك التي ترتكز مصالحها الحيوية على المعلوماتية، وتعتمد عليها في تسيير شؤونها، فقد

(25) دراسة الوضع الراهن في مجال أحكام في المعلوماتية ، إعداد: د محمد القاسم ، د رشيد الزهراني ، د عبد الرحمن السند ، عاطف العمري ، مشروع الخطة الوطنية لتقنية المعلومات ، ص7 ، 6.

تحولت هذه الجرائم من مجرد انتهاكات فردية لأمن النظم والمعلومات إلى ظاهرة تقنية عامة، ينخرط فيها الكثير ممن تتوافر لديهم القدرات في مجال الحاسب الآلي والاتصال بشبكات المعلومات.

إن المقاومة للجرائم والاعتداءات الإلكترونية على نوعين:

النوع الأول: المقاومة الفنية.

النوع الثاني: المقاومة النظامية.

وتتم الحماية الفنية التقنية بعدة وسائل منها:

أولًا: تشفير البيانات المهمة المنقولة عبر الإنترنت.

ثانيًا: إيجاد نظام أمني متكامل يقوم بحماية البيانات والمعلومات.

ثالثًا: توفير برامج الكشف عن الفيروسات والمقاومة لها لحماية الحاسب الآلي والبيانات والمعلومات من الإضرار بها.

رابعًا: عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية، مع عمل وسائل التحكم في الدخول إلى المعلومات والمحافظة على سريتها.

خامسًا: توزيع مهام العمل بين العاملين، فلا يعطى المبرمج مثلًا وظيفة تشغيل الحاسب الآلي إضافة إلى عمله، ففي هذه الحالة سوف يكون قادرًا على

كتابة برامج قد تكون غير سليمة، ومن ثم تنفيذها على البيانات الحقيقية، كما يتم توزيع مهام البرنامج الواحد على مجموعة من المبرمجين، مما يجعل كتابة برامج ضارة أمرًا صعبًا.

الإنترنت ميدان لكل ممنوع، ولا نغالي إذا قلنا: إن التقدم التقني الذي يشهده العالم اليوم، كما أن له من الجوانب الإيجابية ما يصعب حصره، إلا أن جوانبه السلبية تكاد تكون مدمرة، ما لم تكن هناك مقاومة لهذه السلبيات، فمن خلال شبكة الإنترنت يمكن معرفة كيفية صناعة المتفجرات، وغسيل الأموال، وصناعة القنبلة النووية، وسرقة البطاقات الائتمانية، ولقد أظهر تقرير لمركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من الاعتداءات وجرائم الكمبيوتر تعتمد على المؤسسات الأمنية في إجراءات معالجة المعلومات والبيانات الإلكترونية، وتعاون ضحايا جرائم الكمبيوتر مع رجال الأمن، إلى جانب الحاجة إلى التعاون الدولي المتبادل للبحث الجنائي والنظامي في مجال مكافحة جرائم الكمبيوتر، وفي أوروبا قدمت لجنة جرائم الكمبيوتر توصيات تتعلق بجرائم الكمبيوتر تتمحور حول عدد من النقاط منها المشكلات القانونية في استخدام بيانات الكمبيوتر والمعلومات المخزنة فيه للتحقيق، والطبيعة العالمية لبعض جرائم الكمبيوتر، وتحديد معايير لوسائل الأمن المعلوماتي، والوقاية من جرائم الكمبيوتر، الأمر الذي ينبه إلى المعضلة الأساسية في هذا النوع من جرائم الكمبيوتر وهي عدم الارتباط بالحدود الجغرافية، وأيضًا كون التقنية المستخدمة في هذه الجرائم متطورة جدًا،

فالأموال التي يتم استحصالها لعصابة في طوكيو، يمكن تحويلها في ثانية واحدة إلى أحد البنوك في نيويورك، دون إمكانية ضبطها(26).

إن معظم أدوات الجريمة الإلكترونية تكون متوافرة على الشبكة، وهذا الأمر لا تمنعه الأنظمة في معظم الدول، إما لعدم القدرة على السيطرة عليه، أو لأن هناك استخدامات مفيدة لهذه البرامج، فمثلًا هناك عدة برامج لكسر كلمة السر لدخول الأجهزة المحمية بكلمة مرور وهو ما يطلق عليه (CRACKING) وهذه البرامج تكون مفيدة لمن نسي كلمة السر للدخول على الجهاز، أو الدخول على أحد الملفات المحمية، وفي الوقت نفسه يمكن للمعتدي أن يستغل هذه البرامج في فتح جهاز معين بعد معرفة كلمة السر، والدخول على الإنترنت واستغلاله في الاستخدام السيئ، إذن أدوات القرصنة والإجرام متوافرة، لكن الإجرام يكون في الاستغلال السيئ لهذه الأدوات، ويوجد لدى معظم الدول الكبرى أدوات تعقب لمعرفة مصدر مطلق الفيروس مثلا، أو الهجوم على بريد إلكتروني، أو موقع رسمي لإحدى هذه الدول، ولذلك يحرص هؤلاء المعتدون على أن يتم هذا العمل الإجرامي عن طريق أجهزة الآخرين، وهذا يبين أهمية أن يحمي كل واحد جهازه، وأن يحرص على رقمه السري حتى لا يستغل من قبل الآخرين، وينطبق هذا أيضا على أصحاب الشبكات كالجامعات والمعاهد التي توفر

(26) انظر: جريدة الشرق الأوسط ، العدد 8196 ، يوم الاثنين 7 5 2001 ، ص 51.

الإنترنت لمنسوبيها، فقد يستغلها بعضهم لإطلاق الفيروسات أو غيرها من الاعتداءات الإلكترونية.

إن المحافظة على المعلومات من أهم ما تحرص عليه الهيئات والمنظمات والدول، وحتى على مستوى الأفراد، إذ يمكن تعويض فقدان الأجهزة والبرامج، ولكن تعويض فقدان البيانات والمعلومات أو التلاعب بها يعد من الأمور الصعبة والمكلفة، فالمعلومات والبيانات تعد من أهم ممتلكات أي منظمة، لذا يتم السعي للمحافظة على البيانات والمعلومات قدر الإمكان حتى لا يصل إليها أشخاص غير مصرح لهم، ويتم اتباع مجموعة من الإجراءات التي تضمن سلامة هذه المعلومات منها ما يأتي:

1- عدم إلقاء مخرجات الحاسب الآلي، أو شريط تحبير الطابعة، لأن مثل هذه المخرجات قد تحتوي على معلومات مهمة تصل إلى أشخاص غير مصرح لهم الاطلاع عليها، لذا يجب تمزيق المخرجات بواسطة آلات خاصة قبل إلقائها.

2- استخدام كلمات السر للدخول إلى الحاسب الآلي، وتغييرها كل فترة بحيث تعتمد طول الفترة على أهمية البيانات بالنسبة للمنظمة، كما أن بعض أنظمة التشغيل لا تسمح باستخدام كلمة السر نفسها مرة أخرى، وتجبرك على تغييرها بعد فترة محددة من قبل المشرف على نظام التشغيل.

3- عمل طرق تحكم داخل النظام تساعد على منع محاولات الدخول غير النظامية مثال ذلك: عمل ملف يتم فيه تسجيل جميع الأشخاص الذين

وصلوا أو حاولوا الوصول إلى أي جزء من البيانات: يحوي رقم المستخدم، ووقت المحاولة وتأريخها ونوع العملية التي قام بها وغير ذلك من المعلومات المهمة.

4- توظيف أشخاص تكون مهمتهم المتابعة المستمرة لمخرجات برامج الحاسب الآلي للتأكد من أنها تعمل بشكل صحيح، وخاصة البرامج المالية التي غالبًا ما يكون التلاعب بها من قبل المبرمجين أو المستخدمين، وذلك عن طريق أخذ عينات عشوائية لمخرجات البرنامج في فترات مختلفة، كما يقومون بفحص ملف المتابعة للتعرف على الأشخاص الذين وصلوا إلى البيانات، أو حاولوا الوصول إليها.

5- تشفير البيانات المهمة المنقولة عبر وسائل الاتصالات كالأقمار الصناعية أو عبر الألياف البصرية، بحيث يتم تشفير البيانات، ثم إعادتها إلى وضعها السابق عند وصولها إلى الطرف المستقبل، ويتم اللجوء إلى تشفير البيانات والمعلومات إذا كانت مهمة، لأن عملية التشفير مكلفة.

6- عمل نسخ احتياطية من البيانات تخزن خارج مبنى المنظمة.

7- استخدام وسائل حديثة تضمن دخول الأشخاص المصرح لهم فقط إلى أقسام مركز الحاسب الآلي، كاستخدام أجهزة التعرف على بصمة العين، أو اليد، أو الصوت [27].

تحديات مكافحة الجريمة:

تواجه الجريمة التقنية في ظل العولمة الثقافية، تحديات كبيرة في مواجهتها ومكافحتها، نظراً لأساليب التقنية التي تستخدمها من ناحية، وتنوع أشكالها وتعددها من ناحية أخرى. فتلك الجرائم كثيرة ومتنوعة وسريعة، وتشمل كافة نواحي الحياة الاجتماعية والاقتصادية والثقافية وأيضاً الأمنية، مما يجعل هذه الجرائم تمثل تهديداً خطيراً لأمن الفرد والمجتمع والثقافة.

ومن هنا نجد أنه لا يوجد حل جذري ينصح به للوقاية من جرائم الحاسب الآلي بأشكالها المختلفة، فكما سبق أن رأينا، فإن جرائم الحاسب الآلي والإنترنت تتنوع أشكالها وتتعدد أساليب إرتكابها وتظهر في كل يوم أساليب جديدة بحسب التطور التقني الذي يحدث بسرعة رهيبة، في كافة الوسائل والأساليب الاتصالات الحديثة، إلا أنه يجب وضع إستراتيجية أمنية شاملة لنظم المعلومات تحدد عناصرها ومسئوليات الدخول إلى نظم المعلومات، كما

(27) انظر: مقدمة في الحاسب الآلي وتقنية المعلومات طارق بن عبد اللـه الشدي ، دار الوطن للنشر الرياض ، الطبعة الثانية ، 1416هـ ، ص188.

يجب وضع خطة طوارئ دقيقة واختبارها ومراجعتها بصفة دورية. (صالح المسند، 2000م، 190)

أما عن تحديات مواجهة الجريمة الإرهابية التقنية في ظل نظام العولمة، فقد قدم "مارتن نايجمان" M. Nabgman تقريراً حول "أوربا ومجتمع المعلومات العالمي" أو ما يسمي بمجتمع الإعلام الكوكبي، وقد نشر التقرير في يوليو 1994م، وقد تضمن التقرير خطة عمل ضمن أربعة محاور رئيسية، وقد كانت أهم نقطة في التقرير هي "ضرورة سرية البيانات وحماية حقوق الملكية الفكرية". (محمد الرومي، 2003، 112 – 113)

وقد ناقش وزراء خارجية دول الاتحاد الأوربي مشروع يسمح بحماية أسس البيانات، هذا بالإضافة إلى قرارات مؤتمر قمة الدول الصناعية السبعة في فبراير من عام 1995م.

ولمكافحة الجريمة التقنية، وحماية البيانات والمعلومات الإلكترونية، فقد قدم كل من وزير العدل الكندي والنائب العام في نهاية 1995م، قدما مشروع قانون يقترحان فيه ما يقرب من مائة وخمسون تعديلاً في قانون العقوبات والقوانين الأخرى المرتبطة به، والخاصة بالجرائم التكنولوجية، وتزوير كروت الاعتماد والاحتيال، والحصول على خدمات بوسائل تدليسية، وذلك من أجل مكافحة ومواجهة الجرائم الالكترونية، وتشديد العقوبات الخاصة بهذه

الجرائم، نظراً لخطورتها على المجتمع والأمن القومي لكافة المجتمعات.(السيد عتيق، 2002م، 42)

ولما كان لجرائم الإنترنت هذه الخطورة على أمن الفرد والمجتمع، وبخاصة ما يتعلق بحرية البيانات والمعلومات الخاصة بكل فرد أو مؤسسة، وخاصة أن تلك الجرائم تمثل اعتداءاً على النفس والعرض والمال وغيرها. وكذلك ما تمثله هذه الجرائم من تهديد للأمن القومي للمجتمعات على مستوى العالم، ما يتبع ذلك من آثار اجتماعية وثقافية واقتصادية سلبية، وبخاصة أن هناك بعض من هذه الجرائم تمثل اعتداءاً على حياة وأمن واستقرار الأسرة والمجتمع، لأن من بين الجرائم التي ترتكب في هذا الشأن ما يعرض تلك الأسر أو المجتمعات لمشكلات اجتماعية بالغة الخطورة، خصوصاً أنها تمس أعراض هذه الأسر، أو التشهير ببعض أفرادها، وكذلك بث الصور والموضوعات التي قد تتسبب في التفكك الأسري، والخلافات العائلية، والتي غالباً ما تؤدي إلى الانفصال أو الطلاق في كثير من الأحيان.

ولما كان لهذه الجرائم هذا القدر من الخطورة، فإنه كان لزاماً على الجهات الأمنية والتشريعية والقضائية أن تطور أساليبها ووسائلها حتى يمكنها التعامل مع جرائم ثورة المعلومات الحديثة، ومواجهة تلك الجرائم الإلكترونية بأسلوب علمي متطور وغير تقليدي، حتى يمكنها أن تقف أمام تحديات عصر العولمة الثقافية وتكنولوجيا الاتصالات والمعلومات، وذلك في ظل التقدم التقني الذي فتح آفاقاً جديدة، وجلب معه مشكلات ومخاطر جديدة لم نكن

نسمع عنها من قبل، لذلك فإن لم نستطع أن نواجهه هذه المخاطر والتهديدات والمشكلات الناجمة عن هذه الثورة المعلوماتية، ونتعامل معها بكفاءة عالية واقتدار، وأن نطور مؤسساتنا وأنظمتنا، فإن أمننا الاجتماعي والقومي سيكون مهدداً وتصبح بذلك حياتنا الاجتماعية والثقافية والاقتصادية، بل والإستراتيجية في خطر كبير، لذلك يجب وضع البرامج والأساليب والطرق الحديثة الفعالة للتعامل مع هذا الواقع الجديد الذي فرض نفسه على الأفراد والمجتمعات على مستوى العالم كله. (صالح المسند،عبد الرحمن المهيني 2000م، 194)

ورغم أن "الإنترنت" يمكن أن يستفاد منه في فتح آفاق جديدة للمعرفة والتقدم التقني لكافة المؤسسات التعليمية والصحية والاقتصادية، والاستفادة كذلك منه في التسويق والإعلان والخدمات العديدة الأخرى، وهذا هو الغرض الأساسي الذي أنشئ من أجلها، لخدمة البشرية وتيسير الاتصالات الدولية ونقل البيانات والمعلومات التي تعود بالفائدة على الفرد والمجتمع، إلا أنه قد فتح أبواباً خلفية للمتسلين واللصوص لارتكاب العديد من المخالفات والجرائم، وبخاصة تلك النوعية التي تهدد أمن الفرد والمجتمع، أو تلك الجرائم التي تؤثر سلباً على الأمن الاجتماعي والقومي لكافة مجتمعات العالم، وهذه النوعية من الجرائم الإلكترونية تمثل خطراً – ليس كليا بل دولياً – كبيراً يجب التصدي له ومواجهته تتضافر فيه جهود الفرد والمجتمع المحلي وكذلك الدولي نظراً لما تحمله من تهديدات على الصعيدين الفردي والمجتمعي.

وسائل حماية شبكات المعلومات

أولاً: كلمات المرور Pass Words

لكل بيت مفتاح .. هكذا هي فكرة عمل كلمة المرور، فبدونها لا يمكن لأي شخص غير مخول بالدخول على شبكة المعلومات، وهي جواز مرور المستخدم إلى الشبكة، فكلمة المرور تثبت للشبكة بأنك أنت الشخص المخول للدخول إليها، وهي أبسط أنواع حماية المعلومات على شبكة المعلومات فهي تعمل على حماية معلوماتك الشخصية ومعلومات العمل الخاصة بك وسجلاتك الشخصية، وغيرها من البيانات، كما أنها في بعض الأحيان تكون حماية للأفعال مثل كلمة السر في المشتريات والحسابات البنكية وغيرها. ومن أهمية كلمة المرور يجب علينا أن نحرص عليها وعند اختيارها يجب مراعاة مايلي:-

- **اختيار كلمة مرور صعبة ولا يسهل تخمينها.**
- **عدم إطلاع الغير عليها.**
- **تغييرها بشكل دوري.**
- **لا تجعل كلمة المرور كلمة واحدة مثل ragab.**
- **لا تضمن كلمة المرور بيانات شخصية عنك مثل تاريخ الميلاد.**

- **لا ينبغي أن تقل كلمة المرور عن عشرة خانات.**

- **اجعل كلمة المرور خليط بين الحروف والأرقام.**

ثانياً: جدران الحماية Firewalls

يكون جدار الحماية الناري إما برنامجاً أو جهازاً يستخدم لحماية الشبكة والخادممن المتسللين، وتختلف جدران الحماية حسب احتياجات المستخدم، فإذا استدعت الحاجة إلىوضع جدار الحماية على عقدة منفردة عاملة على شبكة واحدة فإن جدار الحماية الشخصي هوالخيار المناسب، وفي حالة وجود حركة مرور داخلة وخارجة من عدد من الشبكات، فيتماستخدام مصافي لجدار الحماية في الشبكة لتصفية جميع الحركة المرورية، علماً بأنالكثير من الشبكات والخوادم تأتي مع نظام جدار حماية افتراضي، ولكن ينبغي التأكد فيماإذا كان يقوم بعمل تصفية فعالة لجميع الأشياء التي تحتاج إليها، فإن لم يكن قادراًعلى ذلك، فينبغي شراء جدار حماية ناري أقوى منه.

وفي بعض الأحيان تقوم بعض شبكات المعلومات بوضع جدران حماية لعزل شبكتها الداخلية عن شبكة الإنترنت، ولا يكون هذا العزل كلياً بالطبع حتى يمكن للمستخدمين الاستفادة من بعض خدمات الإنترنت وفي نفس الوقت منع المخربين من الدخول إلى الشبكة الداخلية أو اختراق أمن وسرية المعلومات على الشبكة.

وتعمل جدران الحماية بطرق متعددة معتمدة على نوع جدار الحماية والشبكة التي تعمل على حمايتها تبعاً لسياسة المؤسسة، ومن أهم هذه الطرق ما يلي:-

أسلوب غربلة مظاريف البيانات المرسلة Packet Faltering.

غربلة المظاريف مع تغيير عناووين المظاريف القادمة من الشبكة الداخلية.

أسلوب مراقبة السياق Stateful Inspection.

وبالطبع فإن هناك العديد من أنواع جدران الحماية التي تلائم كافة أنواع شبكات المعلومات وفقاً لحجم الشبكة والمؤسسة التي تعمل عليها، فهناك جدران الحماية التي تكون للمؤسسات الحكومية والشركات الكبيرة ذات سرعات وقدرات عالية جداً، مثل ما توفره شركة Sisco، كما أن هناك جدران حماية للمنشآت الصغيرة والشركات المحدودة، وهناك أيضاً برامج جدران الحماية التي يتم تحميلها على الحواسيب الشخصية لحماية الجهاز فقط.

ثالثاً: تحويل العناووين الرقمية 13[Network Address Translation]

تقنية NATتعتمد على إعطاء كل حاسوب متصل بالشبكة رقم مميز يختلف عن باقي الأجهزة، وتقوم منظمة Internet Assigned Numbers Authority IANA بإعطاء هذه الأرقام ولا يكون معترفاً بها إلا عن

طريقها، ونظراً لقلة هذه الأرقام فإنه يعطى رقم واحد للشبكة ثم تقوم هذه الشبكة بإعطاء أرقام داخلية للحواسيب المترابطة بها بحيث لا يتكرر أي رقم، وعندما يرغب جهاز حاسوب من الشبكة الداخلية في الاتصال بشبكة خارجية يأتي هنا دور تقنية NATحيث نقوم بتنصيب جهاز حاسوب يلعب دور الوسيط بين الشبكة الداخلية والشبكة الخارجية ويحمل الرقم المعترف به المُعطى من قبل IANAللشبكة الأم، ويكون مهمته تحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي معترف به من قبل IANAومن ثم يقوم بإرسال المعلومات من الشبكة الداخلية إلى الشبكة الخارجية، وكذلك في استقبال المعلومات من الخارج يقوم بعكس الوظيفة وإرسال المعلومات إلى رقم الجهاز في الشبكة الداخلية، وغالباً ما يكون هذا الجهاز الوسيط الذي يقوم بتطبيق تقنية NATإما جدار حماية ناري Firewallأو موزع Router.

وفي هذه الحالة يقوم الجهاز الذي يعمل بتقنية NATعلى أنه جدار حماية ناري بين أجهزة الشبكة الداخلية وأجهزة الشبكات الخارجية الأخرى، فلا يستطيع مستخدمو أجهزة الشبكات الخارجية معرفة العناووين الرقمية لأجهزة الحاسوب في الشبكة الداخلية مما يحد من عمليات الاختراق التي تعتمد على معرفة رقم IPللأجهزة.

رابعاً: التحديث التلقائي Automatic Update

يعد التحديث الدائم والتلقائي للبرامج وأنظمة التشغيل من أهم نقاط حماية أمن شبكات المعلومات، ذلك أن عملية بناء هذه النظم هي غاية في التعقيد ولا تخلو من بعض الأخطاء التي تحدث في فترات البناء وتعمل الشركات عادة على إيجاد التحسينات المستمرة لسد نقاط الضعف في هذه البرامج والأنظمة، وهذه التحسينات تتاح دائماً فيما يعرف بالتحديثات، ومن تاتي أهمية أن يقوم الشخص بعمليات التحديث الدائم للبرامج والأنظمة التي يتبناها في جهازه الشخصي على المستوى الفردي وعلى مستوى البرامج والأجهزة المستخدمة في شبكات المعلومات، ونظراً لصعوبة مطالبة الشركات لمستخدمي هذه البرامج بتحديث البرامج بأنفسهم فإن معظم الشركات المصنعة لهذه البرامج قامت بإضافة خاصية التحديث الآلي والتلقائي لهذه البرامج، ولكي تعمل هذه الخاصية يقوم البرنامج المثبت في الشبكة بالاتصال تلقائياً وعلى فترات معينة بالشركة المنتجة له والقيام بالبحث عن آية تحديثات جديدة وتنزيلها تلقائياً.

خامساً: التشفير Encryption

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام

عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن.

عبارة عن إدخال تعديلات على المعلومات عند إرسالها إلى جهة معينة، أو تحويلها إلى رموز غير ذات معنى؛ حيث عندما تصل إلى أشخاص آخرين لا يستطيعون فهمها أو الإستفادة منها، لذا فهي عبارة عن تشفير وتحويل للنصوص العادية الواضحة إلى نصوص مشفرة وغير مفهومة، وتبنى على أساس أن كل معلومة تحتاج لفكها وإعادتها إلى الوضع الأصلي شفرة.[28]

ويستخدم مفاتيح تشفير **Encryption**النصوص المرسلة وفك الشفرة من قبل صاحبها والمسموح له بتسلمها، وتستند هذه المفاتيح إلى صيغ رياضية معقدة في شكل خوارزميات وتعتمد قوة وفعالية التشفير على نوعية الخوارزميات، ومازالت تلك العملية تتم بواسطة مفتاح سري يعتمد لتشفير النصوص وفي نفس الوقت لفك تشفيرها وترجمتها إلى وضعها الأصلي باستخدام نفس المفتاح السري، وهو ما يعرف بالتشفير المتناظر **Symmetric**، ثم جاء ما يعرف بالتشفير اللامتناظر **Asymmetric** حلا لمشكلة التوزيع الغير أمن للمفاتيح في عملية التشفير المتناظر معوضاً عن

[28] أحمد عبد اللـه مصطفى. حقوق الملكية الفكرية والتأليف في بيئة الإنترنت. - Cybrarian Journal .- ع 21، ديسمبر 2009 .- متوفرة على الرابط. http://journal.cybrarians.info/index.php?option=com_content&view=article&id=487:2011-08-13-20-29-19&catid=144:2009-05-20-09-53-29&Itemid=62.

استخدام مفتاح واحد باستخدام مفتاحين اثنين مرتبطين بعلاقة رياضية عند بنائهما، وهما مفتاحان الأول: المفتاح العام؛ والثاني: المفتاح الخاص[29]

سادساً: التخزين الاحتياطي Backup

النسخ الاحتياطي Backupهو عمل نسخ احتياطية من محتويات الحواسيب أو شبكات المعلومات وحفظ هذه النسخ الاحتياطية في مكان آمن بعيد، بحيث يمكن الرجوع إليها في حالة حدوث أعطال أو حوادث وكوراث للشبكة وتدميرها لأي سبب كان، وعادةً ما يتم أخذ هذه النسخ بشكل دوري وفق النظام المتبع على الشبكة أسبوعياً أو شهرياً أو حتى يومياً، كما أنه في أغلب الأحوال يتم أخذ هذه النسخ بطريقة آلية من النظام نفسه في وقت محدد.

وتعد هذه الطريقة من أهم وأسهل الطرق التي يمكن من خلالها الحفاظ على سلامة المعلومات الخاصة بشبكات المعلومات وخاصة في حالة التدمير الكامل للشبكة أو اختراقها بهدف محو وتدمير البيانات والمعلومات المتاحة عليها، وتكون في هذه الحالة النسخ الإحتياطية هي الملاذ الآمن لمحتويات الشبكات، وأخذ النسخ الاحتياطية من محتويات شبكات المعلومات تعد من أبجديات الأمن والسلامة للمعلومات والشبكات أي أنها من بديهيات العمل في مجال حفظ شبكات المعلومات. ويقدم المختصون بشبكات المعلومات

[29] جنان صادق عبدالرازق. استخدام التكنولوجيا في الحفاظ على أمن المعلومات.- العربية 3000.-

والنظم عدة نصائح يجب على الفرداتباعها عند القيام بعمل نسخ احتياطية من محتوى شبكات المعلومات وهي:-

1- حفظ النسخ الاحتياطية Backupفي مكان بعيد وآمن وسري، ويفضل أن يكون المكان بعيد عن مقر الشبكة الأم أو المؤسسة المالكة للشبكة تفادياً لضياع هذه النسخ في حالة قيام الكوارث الطبيعية في نفس المكان، فيكون قد ضاعت المعلومات الأصلية والنسخ الاحتياطية أيضاً معها.

2- اختيار وسائط تخزين ذات جودة عالية تقاوم عوامل الزمن ولا تتقادم تكنولوجياً بسرعة.

3- القيام بعمليات النسخ الاحتياطي بشكل دوري وفقاًَ للسياسة المتبعة والإجراءات الخاصة بالمؤسسة المالكة لشبكة المعلومات، وفي كل الأحوال ينبغي ألا تزيد المدة عن شهر.

نصائح عامة في متطلبات أمن شبكات المعلومات

1- تحديد سياسات العمل في شبكات المعلومات، بأن يكون واضحاً تمام الوضوح ما هو المسموح به والممنوع فيما يتعلق بأمن المعلومات على الشبكة.

2- توفير آليات تنفيذ سياسات العمل. بأن يكون معروفاً كيفية تنفيذ هذه السياسات وما هي العقوبات التي ستوقع في حالة المخالفة.

3- العنصر البشري. بأن يتولى إدارة وتشغيل شبكات المعلومات عناصر بشرية مدربة ومؤهلة للتعامل مع هذه التكنولوجيا وألا يترك المجال للهواة للعبث بمثل هذه المقدرات الثمينة وخاصة في الأماكن الحكومية والحيوية على مستوى الدول.

4- تغيير الأوضاع الأصلية لمعدات الشبكات. وذلك بأن يتم كل فترة تغيير الأوضاع الأصلية للمعدات Hardwareوالبرامج Softwareالخاصة بشبكات المعلومات كإجراء احترازي كل فترة لمنع الاختراقات الخارجية.

5- المراقبة.يجب أن يكون هناك نوع من المراقبة والمتابعة لأنشطة المعلومات على الشبكة بشكل دقيق ودائم وذلك بهدف اكتشاف أي أنشطة مشبوهة أو حركات غير طبيعية ضمن نطاق الشبكة وتفادي تفاقم الأوضاع.

6- حسن اختيار مواقع نقاط الشبكة.فيجب أن يتم التدقيق جيداً عند اختيار نقاط الاتصال بشبكات المعلومات، وأن تكون هذه النقاط في مواقع جيدة ومؤمنة ومحمية.

7- بروتوكولات التحقق والتشفير.يجب أن يتم تشغيل بروتوكولات التحقق من الهوية وأنظمة تشفير البيانات لتأمين المعلومات على الشبكة، وأن يتم اختيار البرامج ذات السمعة العالمية في هذا الإطار.

المراجع

- أبو الحجاج، أسامة.(1998م). دليلك الشخصي إلى عالم الإنترنت . القاهرة : نهضة مصر.
- ابوزهرة، محمد.(1976م). الجريمة والعقوبة في الفقة الاسلامي. القاهرة : دار الفكر العربي.
- احمد، هلالي عبدالاله.(2000م). تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي. عابدين : النسر الذهبي للطباعة.
- أديب حضور (2007) بين رسوخ الظاهرة ولحظة الحدث : المواجهة بين الإعلام العربي والإرهاب، مركز اسبار للدراسات والبحوث والأعلام، الرياض.

- أديب حضور (2007) بين رسوخ الظاهرة ولحظة الحدث : المواجهة بين الإعلام العربي والإرهاب، مركز اسبار للدراسات والبحوث والأعلام، الرياض.

- أسامة عبد اللـه قايد - الحماية الجنائية للحياة الخاصة وبنوك المعلومات - دار النهضة العربية القاهرة 1994.
- الإستراتيجية العلربية الموحدة للمعلوماتفي عصر الإنترنت ودراسات أخرى (المنظمة اعلربية للتربية والثقافة والعلوم) تونس,1999.
- بحر، عبدالرحمن محمد.(1420هـ). معوقات التحقيق في جرائم الإنترنت : دراسة مسحية على ضباط الشرطة في دولة البحرين. رسالة ماجستير

غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

- البداينة، ذياب.(1420هـ). جرائم الحاسب والإنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (93-124).
- البداينة، ذياب.(1988م). الأمن الوطني في عصر المعلومات. الجزيرة، 9421.
- البداينة، ذياب.(1999م). التطبيقات الاجتماعية للإنترنت، ورقة قدمت في الدورة التدريبية حول شبكة الإنترنت من منظور أمنى، أكاديمية نايف العربية للعلوم الأمنية، بيروت، لبنان.
- تمّام، احمد حسام طه. (2000م). الجرائم الناشئة عن استخدام الحاسب الآلي. القاهرة : دار النهضة العربية.
- جميل الصغير (2002) الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة.
- جميل الصغير (2002) الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة.
- الجنيدي، ماهر (أ). (1999م). النصر للأقوى والأذكى والقذر، مجلة إنترنت العالم العربي، (نوفمبر)، 36.

- حسن صادق المرصفاوي – قانون العقوبات الخاص – منشأة المعارف – الاسكندرية مصر 1991.
- حنفي , محمد : الإنترنت , مكتبة علاء الدين ,الاسكندرية ,2000.
- حنين بوادي (2006) الإرهاب، مكتبة العبيكان، الرياض.
- خالد حنفي محمد (2005) الإنترنت وتصدير الإرهاب، السياسة الدولية، مركز الأهرام للدراسات الإستراتيجية، القاهرة.
- خالد حنفي محمد (2005) الإنترنت وتصدير الإرهاب، السياسة الدولية، مركز الأهرام للدراسات الإستراتيجية، القاهرة.
- د. المستشار عبد الفتاح بيومي : الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، بدون ناشر، طبعه مزيدة ومنقحه،2009.
- د. المستشار عبد الفتاح بيومي :مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مصر، المحلة الكبرى، دار الكتب القانونية، 2007.
- د. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2001.
- د. زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي، بحث مقدم إلي المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 أكتوبر، 1993.

- د. عمر سالم : المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، دار النهضة العربية، الطبعة الأولى، القاهرة، 2000.
- د. مأمون محمد سلامة : الإجراءات الجنائية في التشريع الليبي، الجزء الأول والثاني، منشورات الجامعة الليبية، كلية الحقوق، الطبعة الأولى، 1971.
- د. محمد الأمين البشري : التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر و الانترنت المنعقد الفترة من 1-3 مايو، بكلية الشريعة والقانون بدولة الإمارات 2000.
- د. محمد العريان : الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.
- د. محمد محي الدين عوض : مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) بحث مقدم إلي المؤتمر السادس للجمعية المصرية للقانون الجنائي، المنعقد من 25-28 أكتوبر، سنة 1993.
- د. مدحت رمضان : جرائم الاعتداء علي الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2000.
- د. هدى حامد قشقوش :جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1962.

- د. هشام محمد فريد رستم : الجوانب الإجرامية للجرائم المعلوماتية، مكتبة الآلات الحديثة، 1994.
- د. هلالي عبد اللاه احمد : اتفاقية بودابست لمكافحة الجرائم المعلوماتية (معلقاً عليها)، دار النهضة العربية، الطبعة الأولى، القاهرة، 2007.
- د.احمد السيد عفيفي – الاحكام العامة للعلانية في قانون العقوبات - دراسة مقارنة - - 2001 – 2002– دار النهضة العربية، القاهرة.
- د.جميل عبد الباقي الصغير – الانترنت و القانون الجنائي – دار النهضة العربية - 2001.
- د.هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات،مكتبة الآلات الحديثة،أسيوط،1992.
- داود، حسن طاهر. (1420هـ). جرائم نظم المعلومات. الرياض : أكاديمية نايف العربية للعلوم الأمنية.
- داود، حسن طاهر. (1421هـ). الحاسب وامن المعلومات. الرياض : معهد الادارة العامة.
- الدمينى، مسفر غرم الـلـه.(1402هـ). الجناية بين الفقه الإسلامي والقانون الوضعي. (ط.2) الرياض : دار طيبة للنشر والتوزيع.
- دوفور, أرنود : الإنترنت (ترجمة منى مليحس/ نبال أدلبي) , مركز التعريب والترجمة 1998,.

- الزغاليل، أحمد سليمان.(1420هـ). الاتجار بالنساء والأطفال، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (43-90).
- السيد عتيق (2002) جرائم الإنترنت، دار النهضة العربية، القاهرة.
- السيد عتيق (2002) جرائم الإنترنت، دار النهضة العربية، القاهرة.
- السيد، سمير.(1997م). محاضرات في شبكة المعلومات العالمية. القاهرة : مكتبة عين شمس.
- السيف، محمد ابراهيم.(1417هـ). الظاهرة الإجرامية في ثقافة وبناء المجتمع السعودي : بين التصور الاجتماعي وحقائق الاتجاه الاسلامي. الرياض : مكتبة العبيكان.
- شتا، محمد محمد.(2001م). فكرة الحماية الجنائية لبرامج الحاسب الآلي. الإسكندرية: دار الجامعة الجديدة للنشر.
- الشنيفي، عبدالرحمن عبدالعزيز.(1414هـ). أمن المعلومات وجرائم الحاسب الآلي. (ط1) الرياض : بدون.
- الشهاوي، قدري عبدالفتاح.(1999م). اساليب البحث العلمي الجنائي والتقنية المتقدمة. الاسكندرية :منشأة المعارف.
- صالح الفريح (2007) مواجهة جرائم التطرف والغلو والتفكير من خلال الانترنت، ندوة المجتمع، والأمن، الجرائم الإلكترونية، الرياض

- صالح الفريح (2007) مواجهة جرائم التطرف والغلو والتفكير من خلال الانترنت، ندوة المجتمع، والأمن، الجرائم الإلكترونية، الرياض
- صالح المسند، عبدالرحمن الجهني(2000) جرائم الحاسب الآلي: الخطر الحقيقي في عهد المعلومات، أكاديمية نايف للعلوم الأمنية، مجلدة 15 عدد 29 الرياض.

- صالح المسند، عبدالرحمن الجهني(2000) جرائم الحاسب الآلي: الخطر الحقيقي في عهد المعلومات، أكاديمية نايف للعلوم الأمنية، مجلدة 15 عدد 29 الرياض.

- طارق محمد الجملي، الدليل الرقمي في الإثبات الجنائي، منشور علي مواقع الإنترنت، بدون ترقيم للصفحات.
- طالب، احسن.(1998م). الجريمة والعقوبة والمؤسسات الاصلاحية. الرياض : دار الزهراء.
- عبد الفتاح بيومي (2009) الأحداث والإنترنت : اثر الإنترنت في انحراف الأحداث، دار الفكر العربي، الإسكندرية.

- عبد الفتاح بيومي (2009) الأحداث والإنترنت : اثر الإنترنت في انحراف الأحداث، دار الفكر العربي، الإسكندرية.

- عبد الفتاح بيومي حجازي – جرائم الكمبيوتر والانترنت – دار الكتب القانونية – القاهرة 2005.

- عبد الفتاح بيومي حجازي – جرائم الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – القاهرة 2007.
- عبد المعطي , جمال/وآخرون:الإنترنت والاستخدامات المتطورة,مطابع المكتب المصري الحديث,مصر,2000.
- عبدالرحيم صدقي (1989) الظاهرة الإجرامية، دار الثقافة العربية، القاهرة.
- عبدالرحيم صدقي (1989) الظاهرة الإجرامية، دار الثقافة العربية، القاهرة.
- عبدالعزيز الشبل (2007) الجرائم الإلكترونية نسخ البرامج أنموذجاً، ندوة الأمن والمجمتع، الجرائم الالكترونية، الرياض.
- عبدالعزيز الشبل (2007) الجرائم الإلكترونية نسخ البرامج أنموذجاً، ندوة الأمن والمجمتع، الجرائم الالكترونية، الرياض.
- عبدالفتاح بيومي (2008) عالم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية.
- عبدالفتاح بيومي (2008) عالم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية.
- عبدالمطلب، ممدوح عبدالحميد.(2001 م). جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية : الجريمة عبر الإنترنت. الشارقة: مكتبة دار الحقوق.

- عجب نور، اسامة محمد.(1417هـ). جريمة الرشوة في النظام السعودي. الرياض : معهد الادارة العامة.
- عزالدين، أحمد جلال.(1414هـ). أساليب التعاون العربي في مجال التخطيط لمواجهة جرائم الارهاب. الرياض : أكاديمية نايف العربية للعلوم الأمنية.
- عودة، عبدالقادر.(1401هـ). التشريع الجنائي الإسلامي. بيروت : مؤسسة الرسالة، (المجلد الأول).
- عيد، محمد فتحي.(1419هـ). الإجرام المعاصر. الرياض : أكاديمية نايف العربية للعلوم الأمنية.
- فتوح الشاذلي – القانون الدولي الجنائي – دار المطبوعات الجامعية – الاسكندرية – 2001.
- فرحات، محمد نعيم.(1404هـ). التشريع الجنائي الاسلامي. جدة : مكتبة الخدمات الحديثة.
- الفنتوخ، عبدالقادر.(1421هـ). الإنترنت للمستخدم العربي. الرياض: مكتبة العبيكان.
- فهد بن عبدالـله اللحيدان، – الإنترنت، شبكة المعلومات العالمية - الطبعة الأولى- الناشر غير معروف - 1996.
- القدهي، مشعل عبدالـله. (1422هـ). المواقع الإباحية على شبكة الإنترنت وأثرها على الفرد والمجتمع. [1422/7/29هـ] http://www.minshawi.com/gadhi.htm

- كرودر, ديفيد/كرودر, رواندا: علم نفسك الإنترنت(ترجمة خالد العامري)دار الفاروق،مصر2000.
- كورت, روبرت/ ووترز ,بويد:انترنت (ترجمة خالد العامري)دار الفاروق,مصر2000.
- م.حسن طاهر داوود : جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، 2000.
- الماوردي، محمد حبيب.(1407هـ). الاحكام السلطانية. القاهرة : دار التراث العربي.
- مبدر سليمان لويس – أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية ، رسالة الدكتوراة – حقوق القاهرة.
- مجلة أفاق الإنترنت. (1997)، إنترنت 2، المؤلف، السنة 1 (3)، 38-41.
- محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004.
- محمد امين الرومي(2003)جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية.
- محمد امين الرومي(2003)جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية.

- محمد حسن منصور – المسؤولون الالكترونين – دار الجامعة – للنشر – الاسكندرية 2003.
- محمد سامي الشوا ثورة المعلومات وبعكسها على قانون العقوبات دار النهضة العربية القاهرة 1994.
- محمد عبد الطاهر حسين – المسئولية القانونية في مجال شبكات الانترنت - 2002 – دار النهضة العربية – القاهرة.
- محمد لطفي (2007) الجرائم المعلوماتية: التحديات والحلول ندوة المجتمع والأمن الجرائم الالكترونية، الرياض.
- محمد لطفي (2007) الجرائم المعلوماتية: التحديات والحلول ندوة المجتمع والأمن الجرائم الالكترونية، الرياض.
- محمد، عادل ريان. (1995م)، جرائم الحاسب الآلي وأمن البيانات، العربي، (440)، 73 – 77.
- محمود نجيب حسني – شرح قانون العقوبات – القسم الخاص – الجرائم المضرة بالمصلحة العامة – دار النهضة العربية - القاهرة.
- مدحت رمضان – جرائم الاعتداء على الاشخاص و الانترنت – دار النهضة العربية – القاهرة – 2000.
- مشعل بن عبدالله القدهي (2007) مسح وتحليل ظاهرة تقنية الإنترنت حول العالم مع تحليل الأساليب المتبعة في ذلك، ندوة الأمن والمجتمع الجرائم الالكترونية، الرياض

- مشعل بن عبدالـلـه القدهي (2007) مسح وتحليل ظاهرة تقنية الإنترنت حول العالم مع تحليل الأساليب المتبعة في ذلك، ندوة الأمن والمجتمع الجرائم الالكترونية، الرياض.
- مصطفى موسى (2003) أساليب إجرامية بالتقنية الرقمية : ماهيتها – مكافحتها، دار الكتب والوثائق المصرية، القاهرة.
- مصطفى موسى (2003) أساليب إجرامية بالتقنية الرقمية : ماهيتها – مكافحتها، دار الكتب والوثائق المصرية، القاهرة.
- مصطفى موسى (2005) أساليب إجرامية بالتقنية الرقمية ماهيتها.. مكافحتها دار الكتب القانونية، المحلة الكبرى.
- مصطفى موسى (2005) أساليب إجرامية بالتقنية الرقمية ماهيتها.. مكافحتها دار الكتب القانونية، المحلة الكبرى.
- ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائي – دار النهضة العربية القاهرة 1983.
- مندورة، محمد محمود.(1410هـ). الجرائم الحاسب الآليية، دورة فيروس الحاسب الآلي، مكتب الأفاق المتحدة : الرياض، 19 – 26.
- منصور، عبدالمجيد سيد احمد.(1410هـ). السلوك الاجرامي والتفسير الاسلامي. الرياض : مركز ابحاث الجريمة.
- منير الجنبيهي – ممدوح الجنبيهي – البنوك الالكترونية ط 2 – 2006 دار الفكر الجامعي – الإسكندرية.

- الهادي ,محمد محمد :تكنولوجيا الإتصالات وشبكات المعلومات , المكتبة الأكاديمية , مصر2001.
- هاشم الزهراني (2007) الإرهاب المعلوماتي : المواجهة، كلية الملك فهد الأمنية، مركز البحوث، ندوة المجمتع والأمن الجرائم الإلكترونية، الرياض.
- هاشم الزهراني (2007) الإرهاب المعلوماتي : المواجهة، كلية الملك فهد الأمنية، مركز البحوث، ندوة المجمتع والأمن الجرائم الإلكترونية، الرياض.
- هدى حامد (2000) الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون جامعة الإمارات.
- هدى حامد (2000) الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون جامعة الإمارات.
- يحيى أبو مقايضي (2007) استراتيجيات تقنية لمواجهة الجريمة الالكترونية، نموذج شمولي، ندوة المجتمع والأمن الجرائم الالكترونية الرياض.

- يحيى أبو مقايضي (2007) استراتيجيات تقنية لمواجهة الجريمة الالكترونية، نموذج شمولي، ندوة المجتمع والأمن الجرائم الالكترونية الرياض.
- اليوسف، عبدالله عبدالعزيز.(1420هـ). التقنية والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (195- 233)

الفهرس